CORPORAL MICHAEL J. CRESCENZ
DEPARTMENT OF VETERNS AFFAIRS MEDICAL CENTER
PHILADELPHIA, PHILADELPHIA 19104

MEDICAL CENTER MEMORANDUM NO. 00-17 **JULY 2016**

PRIVACY POLICY

1. **PURPOSE:**

A. This memorandum implements facility privacy policy in compliance with Veterans Health Administration (VHA) Handbook 1605.01, Privacy and Release of Information, and establishes responsibilities and procedures for the privacy protection of information that is accessed, collected, maintained, used, disclosed, transmitted, amended and/or disposed of by the staff and systems of the Corporal Michael J. Crescenz Department of Veteran Affairs Medical Center (CMCVAMC).

B. The components in this policy are designed to meet all of the specific requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and VA/VHA policy. If any of the policy elements contained herein are removed, this facility policy will not be fully compliant.

C. In this document, the term workforce refers to on-site or remotely located employees, residents, students, Without Compensation (WOC) staff, volunteers, and any other appointed workforce members. Contractors will be held responsible for adhering to these policies and procedures in accordance with contracts and Business Associate Agreements (BAA).

2. **POLICY:**

A. This facility will develop, implement, maintain, and enforce a structured privacy program to properly use, disclose and safeguard individually identifiable information. The privacy program is designed to allow continued operation of mission-critical activities while ensuring the integrity, availability, confidentiality, and authenticity of data and information; minimum necessary access to protected health information; and a continuing awareness of the need for, and the importance of, information privacy within the facility.

B. All members of the workforce are responsible for complying with this privacy policy, applicable federal laws and regulations, VA/VHA policies, as well as the procedures and practices developed in support of these policies. All facility privacy policies and procedures must be consistent with VHA Directive 1605, BAA Handbook 1605.05 and VHA Handbooks series 1605.

C. All privacy and other workforce members responsible for implementing and complying with these policies and procedures will be provided copies of, or access to, this policy.

D. Violations of privacy policies or procedures will be brought to the attention of management for appropriate disciplinary action and/or sanctions, and reported in accordance with national and local policy. Privacy violations will be reported through the Privacy and Security Event Tracking System (PSETS) to the VA Network and Security Operations Center (VA-NSOC) by the facility Privacy Officer within one hour of discovery during normal business or outside of normal business hours. After business hours the point of contact is the Administrator on Duty (AOD). The AOD will contact

the Privacy Officer via cell who will submit a ticket with the National Service Desk (NSD) by calling ***(1-855-673-4357 Option 6, Option 1) or sending an encrypted email to NSD.VPNSecurity@va.gov*** . The NSD will open a CA ticket and route it to the NSOC Network Defense Center (NDC), who would then open a PSETS ticket for the PO. The AOD will also prepare a Report of Contact or an encrypted email outlining details of the complaint/incident for submission to the Privacy Officer (PO)/Alternate PO and/or Information Security Officer (ISO) at vhaphiprivacyofficer@va.gov

E. All policies and procedures, and any actions/activities taken as a result of a privacy complaint/violation, must be documented in writing and a written response letter must be given or sent to the complainant. In addition to policies and procedures, privacy-related communications, decisions, actions, and activities or designations, including any signed authorizations, must be documented and kept in a complaint file. All documentation must be retained in accordance with the VA records control schedule (RCS-10).

F. All documentation related to the information privacy program will be reviewed and updated as needed in response to operational changes affecting the privacy of individually- identifiable information (III).

G. Medical Center Director is responsible for designating a facility Privacy Officer and a FOIA Officer in writing. The facility must identify at least one alternate Privacy Officer and FOIA Officer to allow for coverage when the designated Privacy and FOIA Officer is unavailable.

3. **RESPONSIBILITY:**

A. Executive Management (Director, Associate Director, Chief Nursing Executive, Chief of Staff) is responsible for:

(1) Providing the necessary resources (funding and personnel) to support the Privacy Program, maintaining a culture of privacy, and ensuring that the facility meets all the privacy requirements mandated by VA/VHA policy and other federal legislation [e.g., Freedom of Information Act (FOIA) [5 U.S.C.§ 552], Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule [45 C.F.R. Parts 160 and 164], Health Information Technology for Economic and Clinical Health (HITECH) Act, Privacy Act (PA) [5 U.S.C. §552a], VA Claims Confidentiality Statute [38 U.S.C. 5701], Confidentiality of Medical Quality Assurance Review Records [38 U.S.C. 5705], and Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Medical Records [38 U.S.C. §7332]].

(2) Ensuring Privacy Officer coverage for the facility and its associated clinics. It is required by VHA Privacy Policy that the facility Privacy Officer report directly to the Medical Center Director or Associate Director. When the

facility Privacy Officer or Alternate is not available, provide coverage for off-hours operations if conducting 24/7 operations.

(3) Ensuring facility Privacy Officers are fully involved in all projects concerning the access, collection, maintenance, use and/or disclosure, transmission, amendment, and/or disposal of III.

(4) Ensuring that new and revised Memorandums of Understanding (MOU), Contracts, Data Use Agreements (DUA), Business Associate Agreements (BAA), or similar agreements which involve the collection, transmission, use or sharing of information are reviewed by the facility Privacy Officer, in accordance with VA Handbook 6500.6, Contract Security, prior to approval by Executive Leadership.

(5) Ensuring that the facility Privacy Officer is included in discussions and privacy concerns of the facility, which are addressed in strategic initiatives, and maintains a facility culture of privacy.

(6) Cooperating with the facility Privacy Officer in any investigation, mediation strategies, or correspondence that is required in order to investigate and resolve a complaint or allegation.

(7) Certifying annually or on an as needed basis, to the VHA Privacy Office, that privacy training has been completed for all personnel. This shall include all employees, volunteers, contractors, students, residents, and any other person performing or conducting services on behalf of the facility.

(8) Cooperating fully in submissions of Facility Self-Assessments (FSA) and On-site Privacy Compliance Assurance Assessments as required by the Privacy Compliance Assurance (PCA) Office.

(9) Ensuring that facility employees exercise appropriate precautions and safeguards when discussing Veterans' individually identifiable information in public areas, such as clinic waiting rooms.

B. Privacy Officer is responsible for:

(1) Developing, implementing and updating local privacy policies and procedures.

(2) Conducting periodic assessments, compliance reviews and/or audits of the facility's collection, use, storage and maintenance of personal information.

(3) Establishing effective working relationships with the facility Information Security Officer, Facility Chief Information Officer (FCIO), Contracting Officer, Research Compliance Officer, Compliance Officer, and Human Resources

Management personnel to ensure that local policies and procedures which may impact the privacy program support and complement each other.

(4) Ensuring that Executive Leadership is apprised of all privacy related issues.

(5) Coordinating with the facility Information Security Officer for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule, HITECH or other federal privacy statutes.

(6) Serving as the facility's point of contact (POC) for matters relating to the privacy policies and procedures.

(7) Ensuring that members of the workforce receive training and education about privacy policies and procedures as required by VHA Privacy Program.

(8) Ensuring that members of the workforce know whom to contact when a privacy complaint, incident or violation is identified or received.

(9) Monitoring facility and workforce compliance with VHA privacy policies and procedures as well as compliance with local privacy policies and procedures.

(10) Identifying and reviewing areas within the facility for auditory privacy risks, to ensure appropriate safeguards are in place to limit incidental disclosures.

(11) Ensuring processes are in place for the appropriate accounting of disclosures of individually identifiable information made by the facility and appropriate utilization of the ROI Plus software or other tracking mechanism are used in accordance with the facility's policies and procedures. The processes will include accounting for authorizations electronically conducted through iMed Consent.

(12) Collaborating with various program officials and the Contracting Officer, to ensure identification of all entities meeting the definition of Business Associates.

(13) Maintaining a list of active Business Associates utilized by the facility and ensuring all Business Associates have a signed BAA in place prior to disclosure of individually identifiable health information (IIHI) and that the Business Associate adheres to the requirements of the BAA.

(14) Ensuring that the facility does not maintain any unauthorized Privacy Act system of records.

(15) Ensuring all facility developed paper, web-based or electronic forms that collect personal information contain the appropriate Privacy Act statements.

(16) Reviewing and approving all MOUs, Contracts and/or DUAs when required for the sharing of VA sensitive data between the facility and other parties.

(17) Ensuring prompt investigation and follow-up on allegations or known occurrences of privacy violations or complaints including logging the violation or complaint in the Privacy and Security Event Tracking System (PSETS). PSETS should be initiated upon notification of the violation during normal business hours, within one hour of discovery during normal business hours or as soon as possible outside of normal business hours. If a privacy violation presents the risk of media involvement, congressional inquiry, legal action , immediate harm to any individual or any other high-risk outcome, the incident must be reported within one hour of discovery regardless of discovery time (even during non-business hours).

(18) Reports promptly to the VHA Privacy Office any potential privacy complaint, allegation, or activity that has VISN-level or national-level impact.

(19) As a non-voting member of the facility of IRB 1, IRB 2 and CHERP, the Privacy Officer will review all human subject research protocols, exempt and non-exempt, in accordance with VHA Handbook 1200.05 and other applicable guidance to ensure legal authority exits prior to use and disclosure of VHA information for research.

(20) Collaborating with the facility Information Security Officer, FCIO and System Owner to ensure that a Privacy Impact Assessment (PIA) is completed on all information technology systems, applications or programs that collect, maintain, and/or disseminate personally identifiable information (PII).

(21) Reviewing, processing, and monitoring requests to amend any information or record retrieved by an individual's name that is contained in a VA system of records, to include designated record sets, and coordinating such amendments with the author of the document.

(22) Collaborating with the facility Information Security Officer, Contracting Officer Representative (COR) and the Contracting Officer to ensure all contracts are reviewed in compliance with VA Handbook 6500.6.

(23) Ensuring all facility's policies and procedures relating to HIPAA, HITECH, Privacy Act, 38 U.S.C. §5701, §5705, and §7332, and FOIA are consistent with current guidelines and requirements, complementing and supporting each other.

(24) Ensuring local departmental policies and procedures are developed if not specifically outlined in the facility Privacy and FOIA policies.

(25) Provide awareness training through various means for Veterans to inform them of their privacy rights and responsibilities.

(26) Complete the Facility Self-Assessment by the last business day of each quarter or as required by PCA.

(27) Ensuring that the reduction of SSN usage is reviewed to determine the necessity.

(28) Other responsibilities as defined by the VHA Privacy Office.

C. FOIA Officer is responsible for:

(1) Processing all FOIA requests for Federal records that would not otherwise be disclosed in accordance with HIPAA or the Privacy Act, e.g. traditional FOIA requests; requests on deceased veterans; and any request where a no record response is provided.

(2) Ensuring that all FOIA requests or HIPAA/PA requests where information was withheld under a FOIA exemption are entered into FOIAXpress within the same day as receipt.

(3) Other responsibilities as defined by the VHA FOIA Office.

D. Information Security Officer is responsible for:

(1) Coordinating with the facility Privacy Officer for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule, HITECH or other federal privacy statutes.

(2) Coordinating, facilitating, and updating the establishment of information security policies and procedures, to work in tandem with privacy policies and procedures.

(3) Establishing effective working relationships with the facility Privacy Officer, FCIO, Contracting Officer, Research Compliance Officer, Compliance Officer, and Human Resources Management personnel to ensure that information technology (IT) security and HIPAA/FOIA/PA/Federal Information Security Management Act (FISMA) policies and procedures compliment and support each other.

(4) Reviewing and evaluating the security program impact(s) of any proposed facility information privacy policy and procedure changes.

(5) Collaborating with the facility Privacy Officer on addressing/resolving privacy complaints, investigations, and access rights to audits and other information maintained by the facility Information Security Officer.

E. Clinical staff or designees are responsible for:

(1) Reviewing and determining appropriateness for granting individuals' requests for record amendment.

(2) Using and disclosing protected health information only when legal authority exits.

F. Facility Chief Information Officer (FCIO) or designee is responsible for:

(1) Coordinating with facility Information Security Officer and facility Privacy Officer to provide technical advice and other assistance relative to the reasonable safeguards requirements of privacy statutes and regulations dealing with implementation of IT systems, policies and procedures.

(2) Identifying each locally maintained computer system that contains III and providing technical input for various mandated documents, reports, and investigations.

(3) Ensuring all computer rooms meet acceptable reasonable safeguards and that minimum necessary access is maintained.

G. Chief, Human Resources Management Service (HRMS), or designees are responsible for:

(1) Providing consistent and uniform guidance to supervisors and managers regarding personnel actions, sanctions, or other actions to be taken when employees have violated information privacy practices, laws, regulations, policies and procedures, and rules of behavior (see VA Directive 5021).

(2) Providing appropriate information to facility Privacy Officer for completion of PSETS entries in a timely manner regarding mitigation/disciplinary actions.

(3) Coordinating with facility Privacy Officer on the privacy and disclosure of personnel records and other records maintained by HRMS.

(4) Ensuring that personnel records maintained by the HRMS are maintained in compliance with applicable privacy policies, statutes and regulations.

H. VA Contracting Officer/Contracting Officer Representative (COR) is responsible for:

(1) Working in collaboration with the facility Privacy Officer to ensure that privacy responsibilities are listed in all contracts (see VA Directive 6500.6, Appendix C).

(2) Ensuring through the COR that contractors are aware of, and abide by, those privacy responsibilities as stated in contracts with VA and VHA.

(3) Ensuring that Business Associate Agreements are enacted for contracts which the contractor meets the definition of a Business Associate. A BAA should be a separate document from the contract.

(4) Ensuring that contractors receive the appropriate privacy and, if applicable, security training upon initiation of the contract and annually thereafter.

(5) Ensuring that contract performance meets privacy requirements including mediating and/or terminating the contract if information privacy requirements are not being met.

I. Local Managers, Supervisors, and their designees (e.g. ADPAC) are responsible for:

(1) Identifying and protecting all individually identifiable information (III) used by supervised personnel, including contractors and other workforce members.

(2) Ensuring that III, whether computerized or printed, is secured when work areas under their supervision are unattended.

(3) Training new personnel on roles and responsibilities for protecting III.

(4) Identifying functional categories in accordance with facility policy and ensuring VA personnel have only the minimum necessary access level required to carry out their authorized functions or assigned duties and that VA personnel understand what their minimal level of access is.

(5) Ensuring applicable personnel complete the "Information Security and Privacy Awareness and Rules of Behavior" training. If access to protected health information (PHI) is required then "Privacy and HIPAA" training must be completed within 30 days of hire or before access to PHI is given. Training must be completed annually thereafter and documented using the Talent Management System (TMS). Workforce members must be enrolled in TMS through either self-enrollment (e.g. contractors and volunteers) or automatic enrollment upon hire.

(6) Ensuring that all media (paper, electronic, CDs, disks, portable devices,

etc.) with III is disposed of via approved means. Facility staff will use the locked recycling bins provided by Facilities Management to discard all paper records containing sensitive. Electronic media such as computer hard drives, photocopiers, or other biomedical equipment containing PHI and/or PII will be given to the Office of Information and Technology (OI&T) to properly scrub data or remove the hard drive prior to disposing of or returning any leased pieces of equipment. All other electronic media marked for disposal and containing PHI and/or PII will be given to the ISO for appropriate disposal.

(7) Assists the facility Privacy Officer and Human Resource Management Service with the investigation and resolution of privacy incidents involving their employees and/or program(s).

J. Quality Manager serves as Quality Management (QM) Confidentiality Officer and is responsible for coordinating with the facility Privacy Officer on requests for copies of or access to QM documents. The facility Privacy Officer serves as the final approval authority for determining which documents are classified as quality management documents in accordance with VHA Directive 2008-077, Quality Management (QM) and Patient Safety Activities That Can Generate Confidential Documents prior to disclosure. The facility Privacy Officer will work with the FOIA Officer concerning any exception to disclosure under FOIA.

K. Administrative Officer of the Day (AOD) is responsible for resolving and responding to disclosure issues and incident reporting requirements consistent with VHA Directive 1605, VHA Handbooks 1605 series, VA Directive 6500 and VA Handbook 6500 series during non-business hours.

(1) During non-business hours, the AOD will draft a detailed Report of Contact to the PO, including all documents and information disclosed in response to the incident.

(2) The AOD will provide copies of health records to a non-VA providers/hospitals, etc. in response to written requests when the need for information is considered urgent due to health-related care.

(3) The AOD will complete the Accounting of Disclosure sheet for all disclosures made to non-federal agencies during non-regular business hours and provide the list of disclosures per procedure to the ROI department to log into the DSS ROI Plus Program.

(4) For all non-urgent health record requests from non-federal agencies the AOD will collect and forward the requests to the ROI Department for further action during normal business hours.

(5) If the AOD has any concern a privacy violation presents the risk of media involvement, congressional inquiry, legal action, immediate harm to any

individual, or any other high-risk outcome, the AOD will contact the PO who will contact the Pentad and report the incident within one hour of discovery regardless of discovery time.

(6) The AOD or MSA will be required to provide a copy of Notice of Privacy Practices (NOPP) to each of the humanitarian patients treated at the Emergency Department (ED). Obtain a signature from each of the humanitarian patients treated at the ED on VA Form 10-0483, Acknowledgement of the Notice of Privacy Practices, to acknowledge receipt of the NOPP. (See VHA Handbook 1605.04 Notice of Privacy Practices) A copy of the signed VA Form 10-0483 will be sent to the facility medical record file room and scanned into the administrative side of the Computerized Patient Record System (CPRS) medical. record. The AOD will notify the PO at vhaphiprivacyofficer@va.gov by encrypted email when the NOPP has been provided to a Non- Veteran receiving care at the facility and a copy of the signed VA Form 10-0483, will be sent via inter-office mail to scanning unit for record filing.

L. All individuals who have access to sensitive information are responsible for:

(1) Accessing the minimum necessary data for which they have authorized privileges and on a need-to-know basis in the performance of their official VA duties.

(2) Protecting an individual's rights to privacy and ensuring proper use and disclosure of information. All workforce members will be held accountable for compliance with these policies, procedures, and applicable laws.

(3) Appropriately safeguarding printed and electronic individually identifiable information.
(4) Reporting complaints and/or violations of privacy policies or procedures to the facility Privacy Officer immediately upon discovery.
(5) Consulting the facility Privacy Officer and VHA Handbook 1605.01 for guidance in privacy situations not addressed in this document.

4. **PROCEDURES:**

A. **Administrative Requirements**

(1) Compliance with Privacy Policies

a. The facility and its workforce will comply with the contents of this policy, VHA Handbook 1605.01, and all other applicable privacy laws, regulations, and VA policies.

b. The facility Privacy Officer will monitor compliance with this policy through various means, including continuous assessment for privacy compliance.

(2) Documentation

a. This policy and any changes thereto, must be maintained in writing, either on paper or in electronic form, for a period of at least six (6) years.

b. Changes in VHA Handbook 1605.01: When VHA Handbook 1605.01, is updated which necessitates alteration of facility policies and procedures, the local privacy policies and procedures will be revised without delay. The Privacy Officer will review changes and make a determination as to what local policies require either minor or extensive changes. The Privacy Officer will communicate required changes to each respective Service Chief annotating what change needs to take place in what policy. The respective service chiefs will be responsible for submitting their policy revisions to their Pentad member.

(3) Complaint Process

a. All privacy complaints received by the facility are to be referred immediately to the facility Privacy Officer or Alternate Privacy Officer for review and processing.

b. An individual has 3 years from the date of the complaint to request an investigation into the alleged complaint. Health and Human Services, Office for Civil Rights uses this same time frame for their complaints.

c. The facility Privacy Officer or Alternate will enter all facility privacy incidents and complaints, regardless of validity, into the VA Privacy and Security Event Tracking System (PSETS). During business hours the PO will submit the ticket and proceed with the investigation. After business hours the facility uses the process for incident reporting during non-business hours. The AOD will also contact the Privacy Officer via telephone or encrypted email. All incidents must be reported within one hour of discovery to the VA Network Security Operations Center (NSOC) at (1-855-673-4357 Option 6, Option 1) or sending an encrypted email to NSD.VPNSecurity@va.gov.

d. Notice to Privacy Complaints: All individuals filing a privacy complaint, i.e., privacy complainants, will be provided a copy of the Notice to Privacy Complainants at the time of the complaint submission.

i. If the complaint is made verbally, the Privacy Officer, or Alternate Privacy Officer will obtain mailing information in order to send the Notice to the privacy complainant.

ii. The Notice will be mailed to the privacy complainant within 10 working days if the Notice is not given in person to the complainant. A complaint acknowledgement cover letter will be included when the Notice is mailed.

e. The facility Privacy Officer is responsible for:

i. Investigating all complaints regarding facility privacy practices regardless of validity.

ii. All employees are required to fully cooperate with the facility Privacy Officer and/or the VHA Privacy Office throughout the complaint investigation process.

iii. Cooperating with the VHA Privacy Office on all HHS-OCR complaints and all other privacy complaints submitted to VHACO, in addition to providing timely access to complaint investigation files.

iv. Acknowledging receipt of the privacy complainant in writing

v. Communicating with leadership, as appropriate (i.e., Director, VISN, VHA Privacy Office, Office of Inspector General, and Office of General Counsel).

vi. Determining whether or not a complaint is a privacy violation/incident.

vii. Responding as soon as possible or no later than 60 working days, in writing to the complainant when the complaint does not result in an incident

viii. Appropriately notating the privacy complaint/incident in PSETS.

ix. Documenting outcomes of the investigation and provide findings to the supervisor in coordination with other stakeholders (i.e., Human Resources for sanctions or disciplinary actions, union representatives, department heads).

x. Maintaining an administrative file for all complaints by PSETS ticket number or by date.

xi. Trending the types of privacy complaints identified and reports these trends to the facility leadership bi-annually and VHA Privacy Office, upon request.

f. Complaints Identified as Incidents: When the facility Privacy Officer makes a determination during the investigation that a privacy complaint is a privacy violation/incident, the PSETS ticket classification will promptly be changed from a complaint to an incident.

i. When a privacy complaint is made regarding access to a health record and the facility Privacy Officer cannot prove that the access is likely or not likely authorized, the access must be presumed to be unauthorized and will be reported as a privacy violation/incident in PSETS.

ii. All determinations as to whether or not a privacy incident warrants credit monitoring protection services or a notification only letter will be made by the VA Incident Resolution Team and the Data Breach Core Team (DBCT).

iii. The IRT and DBCT will notify the facility Privacy Officer in accordance with VA Directive 6500.2, Appendix C.

iv. When required the notification letter or credit-monitoring letter will be mailed no later than 30 working days from when the incident was reported by the facility Privacy Officer.

g. Administrative Record Keeping: A privacy complaint file containing all of the documentation of the privacy complaint and investigation will be retained by the facility Privacy Officer in accordance with Record Control Schedule (RCS) 10-1, XL III-8, Privacy Complaint File. Documentation will consist of the following:

i. Initial written complainant's concern or a Report of Contact by the facility Privacy Officer, if the complaint is made orally.

ii. Written documentation of all interviews or statements; and

iii. All written correspondence, including e-mails.

h. All complaints (privacy and/or security related) received by the facility from the Department of Health and Human Services (HHS)-Office for Civil Rights (OCR) will be forwarded immediately to the VHA

Privacy Office in VHACO for appropriate processing. The facility does not have authority to respond to HHS-OCR complaints.

i. If an investigation arises as a result of a HHS-OCR complaint, this facility and its Business Associates must permit the Secretary of HHS access to information, during normal business hours, after coordinating with the VHA Privacy Office.

ii. If the facility Privacy Officer receives a HHS-OCR notification letter, this notification letter should be forwarded via encrypted e-mail to the: VHAPrivacyIssues@va.gov outlook mail group.

i. When addressing complaints the facility Privacy Officer should reference resources available at http://vaww.vhaco.va.gov/privacy/ComplaintTracking.htm.

j. When Human Resources are contemplating employee disciplinary action, they should refer to VA Directive 5021 and VA Handbook 5021, Employee/Management Relations.

k. The facility may not retaliate against a person for exercising rights provided by the HIPAA Privacy Rule, for assisting in an investigation by HHS-OCR or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates these provisions.

l. The facility may not require an individual to waive any right under these provisions as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

(4) Reasonable Safeguards

a. All facility workforce members shall ensure that appropriate administrative, technical, and physical safeguards are used to maintain the security and confidentiality of III, including protected health information (PHI), and to protect against any anticipated threats or hazards to their security or integrity. The facility's personnel shall make reasonable efforts to limit III to the minimum necessary to accomplish the intended purpose of any use, disclosure, or request. This does not pertain to the treatment provision under the HIPAA Privacy Rule.

b. All personnel may access and use information contained in VHA records as required for their official duties related to treatment, payment, and health care operations purposes.

c. When disclosing VHA information, all applicable laws and regulations are reviewed and applied to the request in order to assure utilization of the most stringent provisions for all uses and/or disclosures of data in order to provide the greatest rights to the individual and the minimum necessary of III. III disclosure is mandatory with a valid written authorization, signed by the individual but disclosure must be limited to only the information necessary to satisfy the purpose of the request.

d. Disposal of Paper Documents: Staff disposes of paper documents that contain III by utilizing the recycling bins provided by Facilities Management throughout the hospital and out buildings. These bins are emptied and shredded on site per VHA requirements by a local contractor who will then take the shredded material to be pulverized. When shredding VA sensitive information, only VA approved shredders can be utilized. Final destruction certificates are received and on file with the facility.

e. Disposal of Electronic Media: Electronic media containing III will be destroyed in accordance with the Information Security Office's SOP. Personnel in possession of the electronic media will send an Outlook message to the ISO stating that the media is approved to be destroyed and must have their Supervisor's concurrence on the message. Personnel will follow guidance as directed by the ISO.

f. Disposal of Non-paper Items: Non-paper items (i.e. I.V. bags, wristbands, prescription bottles, etc.) containing III are destroyed by removal of III from the non- paper item and the III destruction disposal will be followed by using the destruction of paper items processes. When de-identifying of non- paper items is not applicable, destruction will be carried out by incineration or shredding.

g. Maintaining Auditory Privacy: Staff only discusses patient care issues in appropriate areas, which allow the maintenance of auditory privacy. Facility staff does not discuss patient information in areas not conducive to confidentiality (e.g., canteen, elevators, or hallways). Signs must be posted alerting Veterans to auditory privacy concerns in waiting areas. VHA health care providers and staff must refrain from discussing patient information within hearing range of anyone who is not on the patient's treatment team or does not have a need to know the specific patient information unless an emergent condition arises whereby auditory privacy cannot be maintained. Administrative staff should follow the same guidance in any discussion involving individually identifiable sensitive information, i.e. employee health or disciplinary actions. Appropriate safeguards include training all staff on auditory privacy to include:

i. Using the Veterans Health Identification Card (VHIC) for identification upon check-in, if available;

ii. Using an appropriate tone of voice when speaking with the Veteran in a public area or during check-in;

iii. Only discussing the information necessary to accomplish the function; for example, not asking for the full Social Security Number (SSN) when the last four of the SSN is sufficient;

iv. Asking other Veterans in line for clinical check-in to wait a short distance away from the desk to allow a zone of audible privacy as opposed to being right behind the Veteran being assisted;

v. Only calling Veterans back to an exam room, pharmacy window or other treatment area by name; and

vi. Going behind closed doors to have discussions pertaining to the personal information of the Veteran.

h. Use of Facsimile (Fax): When using fax technology, facility staff adheres to VA Handbook 6500, Information Security Program; VHA Handbook 1907.01, Health Information Management and Health Records; and this VHA 1605.01, Privacy and Release of Information.

i. III is only transmitted via facsimile (fax) when absolutely necessary. Any disclosure of faxed information containing or requesting individually identifiable patient information must be accounted for in the ROI Plus software or on a manual spreadsheet.

ii. Any staff member utilizing fax as a means of transferring III must take the following steps to ensure that III is sent to the appropriate destination and not to a machine accessible to the general public:

1) Verify the fax number prior to sending the fax and, in order to prevent misdialing, do not use pre-programmed numbers unless the number is tested prior to faxing. Periodically verify the fax numbers of frequent recipients. Ask those frequent recipients to notify the facility of any fax number changes.

2) A fax cover sheet with an appropriate confidentiality statement, instructing the recipient of the transmission to notify the facility if received in error, must be sent with all outgoing faxes. PHI should never be placed within the fax cover sheet as this negates the

confidentiality statement on a fax coversheet. However, the Veteran's name may be referenced in the subject line.

3) For example when transmitting outside VA:

"This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above."

4) Notify the recipient before sending the fax in order to ensure that someone is present to receive the information or that the fax machine is in a secure location (e.g. locked room).

5) Review the fax confirmation slip to verify that the confidential information went to the proper destination number. If there has been an error, immediately contact the incorrect recipient and request return or destruction of the fax.

i. Electronic mail (e-mail) and information messaging applications and systems are used as outlined in VA policy (VA Directive 6301 and VA Handbook 6500). These types of messages never should contain III, unless the authentication mechanisms have been secured appropriately (see VA Handbook 6500). Responding to a patient via email, which contains protected health information, should be done through My Health**e**Vet Secure Messaging.

j. Mailing of Sensitive Information. Mailing of Veteran's correspondences such as copies of records, appointment letters may be done so using the United States Postal Service. Envelopes, parcels, packaging or boxes containing sensitive information must be secured in a manner that prevents unauthorized access, tampering, or accidental loss of contents. Window envelopes must show the recipients' names and addresses, but no other information. (See VA Directive 6609)

k. To the extent practicable, this facility mitigates any harmful effect known to have resulted from an improper use or disclosure of III. Mitigation may include, but is not limited to: operational and procedural

corrective measures; re-training, reprimanding, or disciplining workforce members; addressing problems with any involved business associates; incorporating the chosen mitigation solution(s) into facility procedures. During business hours, VA workforce will report improper uses or disclosures of III or any other privacy incident to the PO, Alternate PO and/or ISO (if applicable). The employee will contact the PO, Alternate PO and/or ISO (if applicable) by preparing a Report if Contact or encrypted email outlining the details of the improper use or disclosure.

(5) Sanctions

a. All individuals who use or have access to VA information systems or sensitive information must sign and adhere to the Rules of Behavior, which bind them to the legal and moral responsibility of preventing unauthorized disclosure. (See VA Handbook 6500, Information Security Program) This facility has established sanctions, which are applied against members of its workforce as appropriate, for failures to comply with privacy policies and procedures and Rules of Behavior.

b. This facility has established a set of rules that describes the information privacy operations of the facility and clearly delineates the responsibilities and expected behaviors of all workforce members. These rules address all significant aspects of using III and the consequences of inconsistent behavior or non-compliance. The entire workforce of this facility will have access to a copy of these rules for purposes of review. A signed (manually or electronically) acknowledgement of these rules is necessary for each workforce member.

c. The facility Privacy Officer will determine information privacy violations and provide evidence thereof. The employee's supervisor will determine appropriate actions and may, in conjunction with human resources management, take necessary steps and apply appropriate sanctions for any employees who are non-compliant with privacy policies and procedures. Penalties will be assessed against any individual(s) who knowingly and/or willfully use, disclose, or obtain information without the individual's written authorization or not as authorized by law.

d. Appropriate legal authorities outside of VHA may levy civil or criminal sanctions for privacy violations. Depending on the statute, penalties range from $50,000 and/or one year in jail to $250,000 and/or up to ten years in jail, per offense. If a penalty is levied, the offending employee, not VA, is responsible for payment. In addition, other adverse actions, administrative or disciplinary may be taken against employees who violate the statutory provisions. Under the HITECH Act, applicable to violations occurring on or after February 18, 2009, the Secretary of Health and Human Services can impose civil monetary penalties for each

violation ranging from at least $100 to a maximum of $50,000 for the lowest category violation. Under the highest category violation, the Secretary can impose a $50,000 penalty per violation. Additionally the HITECH Act increases the maximum penalty that the Secretary of HHS can impose for all such violations of the same HIPAA provision in a calendar year from $25,000 to $1,500,000.

e. Adverse actions may include, but are not limited to, progressive discipline. The facility will follow processes and procedures outlined in VA Handbook 5021 for adverse actions in compliance with the stated Table of Penalties.

(6) Privacy Training and Education

a. The facility Privacy Officer, in coordination with the facility Education Coordinator or Education Office, is responsible for developing a local-level privacy training policy that outlines the facility procedures for ensuring compliance with the annual privacy training requirement of VHA Directive 1605 and VHA Handbook 1605.01.

b. All new employees will complete the assigned VA Privacy and Information Security Awareness course regarding VA Privacy and Information Security Awareness and Rules of Behavior within 30 days of hire and annually thereafter.

c. The facility Privacy Officer will conduct privacy training at all facility New Employee Orientation (NEO) programs.

d. Employees are responsible for annual completion of their mandatory privacy training requirement prior to or on their anniversary date of privacy training the following year.

e. Residents and students must complete their TMS module prior to beginning their rotation at the facility. Residents and students must present a certificate of completion to receive access to the VA systems and begin their Philadelphia rotation.

f. Volunteers complete the TMS module prior to starting their volunteer work at the facility.

g. Part-time employees, contract staff, and WOC staff establish TMS accounts through their services and primarily complete the training through the assigned TMS online modules, but may also use the print version. Certificates of completion for this training are required prior to receiving access to the VA systems

h. The facility Privacy Officer is responsible for developing a local training strategy in conjunction with the facility Education Coordinator or Education Office. Compliance will be monitored by the PO, ISO, Service Chiefs, and facility executive leadership. TMS sends automatic reminders to the individuals and their supervisors 30 days and 15 days prior to the due date for the required training. The health care facility Director will make the strategy available to the VHA Privacy Office upon request.

i. The facility Privacy Officer, in coordination with the facility Education Coordinator, TMS Coordinator or Education Office, shall maintain a process of compiling annual training records in order to report the facility privacy training completion status to the VHA Privacy Office and to the health care facility Director upon request.

i. The annual training records of completion of privacy training must be kept for all workforce members to include the following; employees, volunteers, students, and contractors in order for reporting of facility privacy training completion numbers by each group.

ii. The facility Director will certify annual training completion to the VHA Privacy Office for all work force members based on the reports generated by the health care facility Privacy Officer and Education Coordinator, TMS coordinator or Education Office upon request.

j. The facility Privacy Officer shall conduct other activities within the facility to enhance awareness of privacy and that have a positive impact on the overall privacy culture and posture of the facility. These activities shall include, but are not limited to, participation in VA's annual Privacy Week activities, posting privacy posters and announcements throughout the facility, and conducting one-on-one training with personnel who have been observed displaying negative privacy culture behaviors.

B. **Individual Rights**

(1) Verification of Identity

a. In order to receive or view information from his or her VHA record, an individual must present staff with adequate information for verification of identity. Individuals may not verify identity by email.

b. A Veteran Health Identification Card (VHIC), passport, driver's license, or employee identification card may be used to identify an individual who appears in person. Mail or fax identification requests may be verified by social security number, address and signature comparison to the VHA record.

c. This facility shall recognize legally designated personal representatives as the individual when the individual is unavailable or unable to act on his/her own behalf. Staff should recognize the following representatives of the individual:

i. Legal Guardian: A person designated by a court of competent jurisdiction to manage the property and rights of another person who, due to defect of age, medical condition, understanding, or self-control, is considered by the court to be incapable of administering the individual's own affairs. Depending on the circumstances, the court may appoint a legal guardian for a specific purpose (NOTE: A VA Federal fiduciary is not a legal guardian). Three of the most common types of guardianships are: Legal Guardian of the Person; Legal Guardian of the Property; and Legal Guardian of the Person and Property.

ii. Power of Attorney (POA): All POA's are to be referred to Social Work for determination that the POA meets the legal requirements for making disclosure decisions.

d. A personal representative of a deceased individual is a person, who under applicable law has authority to act on behalf of the deceased individual. This may include power of attorney (if binding upon death), the executor of the estate, or someone under federal, state, local or tribal law with such authority. The next of kin of a deceased individual is considered a personal representative of the deceased individual but not of a living individual. They are recognized as having the same rights as the deceased individual. When there is more than one surviving next-of-kin, the personal representative will be determined based on hierarchy: spouse, adult child, parent, adult sibling, grandparent, or adult grandchild.

NOTE: Regardless of the type or source of the POA presented, the reviewer must always carefully check the document with General and Special Powers of Attorney. The document must be: in writing; signed by the individual giving the power; dated; notarized and signed by a licensed notary public; and specifically designate, by name, the third party agent, which may be an organization or entity, to act on behalf of the individual.

(2) Right of Access

a. If access is legally appropriate, individuals may obtain a copy of, or inspect their record or III. A request to obtain a copy or inspect their record or III must be made in writing by the individual or a personal representative. Individuals may use VA Form 10-5345a, Individuals

Request for a Copy of their Own Health Information, to accomplish this purpose.

b. All requests for copies of individuals' own health information will be directed to the Release of Information Department. All requests must show date received whether by use of a date stamp, writing date received on request, or entering the request in the ROI Plus software the exact same day as received in person or mail.

i. When an individual requests their Sensitive Patient Access Report (SPAR) and does not give a period of time for the running of the report, the VHA healthcare facility Privacy Officer should ask the individual for the timeframe desired. If the individual wants the SPAR for the entire timeframe for which it exists, then it would be provided as such under Right of Access.

c. If the individual or the individual's representative is not entitled to the records under any legal provisions, the facility will not provide him or her with a copy of the records. **NOTE**: this is an infrequent occurrence.

d. Access to view a record must be processed as follows:

i. When individuals appear in person at a VA health care facility, they must be advised at that time whether the right of access or review of records can be granted. When immediate review cannot be granted due to staffing or availability of records, necessary arrangements must be made for a later personal review, or if acceptable to the individual, the copies may be furnished by mail.

ii. Mailed requests must be referred to the facility Privacy Officer or Chief of Health Information Management for determination if the right of access by review will be granted.

1) If additional information is required before the request can be processed, the individual requesting review of the records must be advised.

2) If it is determined that a request to review will be granted, the individual must be advised by mail that access to view the records will be given at a designated location, date and time in the facility, or a copy of the requested record will be provided by mail, if the individual has previously indicated or has been contacted to verify that a copy of the record will be acceptable.

e. All right of access requests, granted requests, denials and adverse determinations are documented in the ROI Plus software, in accordance with VHA Directive 2011-010, Mandated Utilization of Release of Information (ROI) Manager software. Departments within the medical center that provide copies of their own information to outside non-VA entities are required to track the name of requestor and address, if known; the name of individual to whom the records pertain to; what information was disclosed, and the date of disclosure either on the facility spreadsheet or through the ROI Plus software. A copy of the request must be maintained within the department along with their response letter. This information must be maintained for six years or the life of the record and provided to the PO or HIM Chief upon request.

(3) Notice of Privacy Practices

a. An individual will be provided with a copy of IB 10-163, Notice of Privacy Practices, by this facility upon verbal or written request. All Veterans receive a copy of this notice from the Health Eligibility Center (HEC) upon enrollment.

b. An individual may obtain a copy of IB 10-163, Notice of Privacy Practices, from the Health Administrations Services Admissions Department or the Privacy Office. An individual may obtain a copy of the NOPP from any employee who has access to the HAS SharePoint site.

c. A Non-Veteran who receives care and treatment at a facility whether for humanitarian purposes or enrolled in a VA research study must be given a copy of the Notice of Privacy Practices. The HAS admissions clerk is responsible for giving non-veterans a copy of their Notice of Privacy Practices during the registration process. If the non-veteran is participating in a VA research study, the principle investigator or research coordinator is responsible for giving the non-veteran a copy of the Notice of Privacy Practices. HAS and research departments will ensure the Notice of Privacy Practice is scanned into CPRS and the Privacy Officer is notified. See VHA Handbook 1605.04 for further information

d. In an Employee Health situation, an Employee Health staff member may maintain a copy of the acknowledgment form in a binder or in the blue employee health folder if applicable. CPRS should be used only if there is not another place to keep the acknowledgement form.

e. The facility must also establish a process to monitor this requirement to ensure compliance with the rules. The privacy officer will review Humanitarian services report to ensure process is followed using the statement of practice (PRIV 03). The PO will conduct random audits in

each area responsible to ensure ongoing compliance. See VHA Handbook 1605.04 for further information

(4) Amendment Request

a. An individual has the right to request an amendment to any information or records retrieved by the individual's name or other individually-identifiable information contained in a VA system of records, as provided in 38 CFR 1.579 and 45 CFR 164.526. The right to seek an amendment of this information or records is a personal right of the individual to whom the record pertains. The personal representative of a deceased individual has a right to request an amendment of the decedent's records.

b. The amendment files must be maintained for the life of the record. The amendment files are not scanned into the Veteran's health record as they are not considered part of the health record. They may be maintained in a secure and locked file cabinet or scanned to a secure network drive but cannot be scanned into the administrative portion of VistA Imaging in the health record.

i. The amendment file must be retained and destroyed in accordance with the Record Control Schedule (RCS) 10-1, Privacy Amendment Case File under Section XLIII-6.

c. The request must be delivered to the Privacy Officer in order for a date to be placed on the request. If the request is given to staff members other than the Privacy Officer they will forward the document to the PO by interoffice mail using a Sensitive Envelope.

d. Requests to amend records are acknowledged in writing within 10 working days of receipt and if a determination cannot be make within this time period the individual is advised of when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request. The Privacy Officer will acknowledge the request and subsequent notices in writing.

e. The Privacy Officer refers the request and related record to the health care provider who authored the information in order for the provider to determine if the record needs to be amended as requested.

f. When an amendment is approved, the following actions are taken:

i. Any information to be deleted must be made illegible, e.g. marked through, in the paper record. For electronic health records, the facility Privacy Officer or Chief, Health Information Management (HIM) is required to use the Computerized Patient Record System (CPRS) Text Integrated Utility (TIU) functions for amending documents. For all other records, the facility Privacy Officer will work with the responsible record custodian to amend their records, e.g. police or employee records.

ii. Any new material must be recorded on the original document. The words "Amended-Privacy Act, Amendment Filed, and/or 45 CFR Part 164" must be recorded on the original paper document. The new amending material may be recorded as an addendum if there is insufficient space on the original document. The original document must clearly reflect that there is an addendum and care must be taken to ensure that a copy of the addendum accompanies the copy of the original document whenever it is used or disclosed. The amendment must be authenticated with the date, signature, and title of the person making the amendment.

iii. For an electronic amendment of a TIU (Text Integration Utility) document, the Chief of Health Information Management (HIM), or designee, is responsible for utilizing the TIU AMEND action for all TIU documents. Please refer to the TIU User Manual for specific instructions on utilizing the TIU amend functionality found on the HIM website. If the original document cannot be amended and an addendum cannot be attached, then a link to the location of the amendment must be provided. Refer to Non-TIU Document Changes and Corrections Frequently Asked Questions (FAQ) for processes to correct Non-TIU documents.

iv. The individual making the request for amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The Chief of HIM, or designee, or the facility Privacy Officer, or designee, must notify the individual so that they can identify and agree to have us notify any relevant persons or organization that had previously received their information. If 38 U.S.C. § 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations.

v. If the record has been disclosed prior to amendment to a business associate, the business associate must be informed of the correction and provided with a copy of the amended record.

g. When a request to amend a record is denied, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must promptly notify the individual making the request of the decision. The written notification must:

i. Reason for the denial (i.e. information was not created by VHA; information is accurate, relevant, complete or timely in its current form; or information is not part of a VHA system of records or designated record set);

ii. Advisement of appeal rights (the individual may appeal to the Office of General Counsel (024), 810 Vermont Avenue N.W. Washington, DC 20420). If the General Counsel sustains the adverse decision, the individual must be advised, in the appeal decision letter, of the right to file a concise written statement of disagreement with the VA health care facility that made the initial decision.;

iii. Instruction that if an appeal is not filed, the individual has the right to request the VA Medical Center to provide a copy of the initial request for amendment and the subsequent denial with all future disclosures of information.;

iv. Instruction that the individual may also provide a statement of disagreement to the facility and request that the facility provide the statement of disagreement with all future disclosures of the disputed information;

v. Instruction that the individual may complain about the denial to VHA Privacy Office or to the Secretary, Health and Human Services;

vi. The name or title and telephone number of the person or office of contact; and

vii. The signature of the facility Director or the Privacy Officer under approved delegation to sign amendment denials.

h. If requested by the individual, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must identify the individually-identifiable information that is the subject of the disputed amendment and

append or otherwise link the individual's request for an amendment and the facility's denial of the request to the individual's record.

(5) Confidential Communications Request

a. An individual's oral or written request to receive any or all types of communications (correspondence) from facility staff via a confidential alternative means, or at an alternative location, must be processed in accordance with VHA Directive 1067, Confidential Communications or subsequent directive.

b. All confidential communications requests will be referred to Registration under Health Administration Services.

c. When the Veteran makes the request of a staff member to allow for the receipt of written communications at an alternative address other than the permanent address of record:

i. Veterans must specify a start date for use of the confidential correspondence address. Dates occurring in the past are not acceptable. Veterans may specify an end date for use of the address, but it is not required.

ii. The staff member must access the Load/Edit Patient Data menu option and answer the prompts. VistA allows the capture of the new confidential communications address fields including date started and stopped, street address, city, state, zip code including the four digit geocode, and country.

d. If the confidential communications data is on file for the Veteran, that address is used for the mailing of all communications under a specified correspondence type (see VHA Directive 1067, Attachment A, for definitions of the five correspondence types for Health Insurance Portability and Accountability Act (HIPAA) Confidential Communication).

e. Requests to split communications under a correspondence type are considered unreasonable and will be denied. With an exception to My Health**e**Vet, a request to receive communications via electronic mail is also to be considered unreasonable and will be denied.

f. The confidential communications address and correspondence type is transmitted nightly to the Austin Information Technology Center (AITC).

g. A confidential communications address that results in undeliverable mail is considered invalid; and the correspondence is resent or re-mailed to the Veteran's permanent address as notated in VistA.

h. When a confidential communications address is activated for health records, the address is viewable through the ROI Plus software for utilization by the ROI Clerks. ROI Clerks must use the confidential communications address when activated to provide individuals with copies of their own records regardless of the address on the request without further communication with the individual and subsequent change within VistA.

(6) Restriction Request

a. An individual's requests for restrictions on the use or disclosure of his or her Individually Identifiable Health Information (IIHI) that is used to carry out treatment, payment, or health care operations are referred to the facility Privacy Officer. All restriction requests must be made in writing.

b. All requests for restrictions of individually identifiable health information need to be reviewed on a case-by-case basis by the facility Privacy Officer. If the facility is considering granting the request, the VHA Privacy Office should be consulted. Restriction requests are not considered unless they meet the following criteria:

i. Submitted in writing;

ii. Identify which information is to be restricted;

iii. Identify who the information is to be restricted from;

iv. Indicate for what purposes (e.g. use for payment) the identified information is to be restricted; and

v. Be signed and dated by the individual to whom the record pertains.

1) Although this facility is not required to agree to restrictions requested by individuals on behalf of VHA, any restriction granted must be appropriately documented. If a request for restriction is granted, all VHA programs and employees must adhere to the restriction unless the information covered by the restriction is needed to provide a patient with emergency treatment. If a restriction request is granted, it should be entered into the ROI Plus software

under "alerts." This software option is designed to notify only facility ROI clerks that certain portions of a Veteran record should not be disclosed. Notification to the current treatment team and with other VA personnel should be documented by the PO based on the specific access restriction.

c. When a restriction request is denied, the facility Privacy Officer promptly informs the individual of the decision. The notification includes the reason for the denial and the signature of the facility director or designee. All restriction requests and denials are documented and retained by the Privacy Officer. There are no appeal rights given for a denial of a restriction request.

d. A facility has a right to terminate a restriction request. A facility may terminate a restriction, if it informs the individual in writing that it is terminating its agreement to a restriction and that such termination is only effective with respect to protected health information created or received after VHA has so informed the individual.

NOTE: A facility health care provider may NOT grant a restriction request. A verbal request by the Veteran to not share his/her information is not a restriction request. The provider must refer the Veteran to the Privacy Officer for consideration. Provider education is done through e-mails, articles in the Medical Center weekly Pulse and correspondence with Service Chiefs and presentations at staff meetings.

(7) Facility Directory Opt-Out

a. Individuals may request exclusion from the Facility Directory during each inpatient admission, in accordance with the Chief Business Office Procedure Guide 1601B.02. The facility Directory Opt-Out provision does not apply to Emergency Rooms unless the patient is going to be admitted to an inpatient setting. The facility Directory Opt-Out provision does not apply to Outpatient clinics.

b. Upon admission, VistA will prompt the user to select either opt-in or opt-out for each inpatient in the facility directory. During the admission screening process, Admissions clerk must ask each inpatient to specify whether he or she wishes to be excluded from the facility directory and document his/her decision in the VistA system at each admission episode. Clerk will have veteran sign directory form verifying their decision. Form will be scanned into veteran record. If veteran unable to sign form provider will complete the process.

c. VistA should be edited utilizing either the Admit a Patient or Extended Bed Control options to indicate the patient's preference.

d. Each patient must be advised that if they request to be excluded, medical center staff will not be permitted to provide any information to visitors or callers concerning whether a patient is an inpatient at the facility. This includes family, friends, colleagues, deliveries (i.e., flowers, cards, etc.), receipt of mail, or anyone asking about the patient.

e. A patient may, at any time during an admission, change the initial decision to be included or excluded from the facility directory.

f. If an inquiry is received concerning a patient who elects to opt-out of the facility directory, the sample response may be "I am sorry, but I do not have any information I can give you on whether John Q. Veteran is a patient."

i. When a telephone or in-person inquiry is received from a member of the public who is inquiring about a current inpatient, the staff member must first check the VistA options (Patient Inquiry, Inpatient Listing, or Inpatient Roster). Staff must verify caller to see if they are listed as the caregiver or emergency contact. If not listed refer the caller to speak with the family directly for information.

g. If the patient is incapacitated or unable to make this decision at the time of admission, the facility health care provider admitting the patient makes a determination based on the patient's prior admissions and the best interest of the patient.

i. The provider must document this decision in the patient's medical record in CPRS.

ii. Once the patient is able to communicate or make the facility directory opt-out decision, the patient must be given an opportunity to do so. The medical provider must communicate with the veteran to confirm decision.

iii. Employee education relating to the opt-out process will be provided by the Service Line supervisors or designee. The PO will provide education relating to the opt-out process during new employee orientation and through the Privacy Corner in the Pulse. In addition, all employees have unlimited access to the privacy policy on the Intranet.

(8) Accounting of Disclosures

a. The facility maintains an accounting of all disclosures of III for six (6) years after the date of disclosure or for the life of the record, whichever is longer. (See RCS10-1 for additional guidance or your Records Control Officer) This accounting includes disclosures made with or without patient authorization. Disclosures of data to VHA employees performing their official duties in regards to treatment, payment and health care operations and disclosures of de-identified data do not require an accounting.

b. In most circumstances, the accounting will be maintained electronically via the most current version of the ROI Plus software as part of the record from which the disclosure was made. See VHA Directive 2011-010, Mandated Utilization of the Release of Information Records Manager software.

c. For those departments within the VA health care facility that do not utilize the ROI Plus software such as Human Resources, Research, Social Work, Police and Security, Credentialing and Privileging, Employee Health, Non Purchased Care, MCCR, Quality Management and Infection Control As long as the Privacy Officer has approved the tracking system in writing to ensure all required elements of collection and retention are present and the accounting can be retrieved by the Privacy Officer upon request by the patient. All required information fields must be completed in detail for all accounting of disclosure tracking systems using the statement of practice.

d. An individual may request a copy of an accounting of disclosures from his/her records. The request must be made in writing, and adequately identify the system of records or designated record set(s) for which the accounting is requested. The request must be delivered to the facility Privacy Officer so that a date can be put on the request for processing and completion within the 60 calendar days.

e. Accountings must contain the name of the individual to whom the information pertains, date of each disclosure; the nature or description of the disclosed information; a brief statement of the purpose of each disclosure, or in lieu of such statement, a copy of a written request for each disclosure; and the name and, if known, address of the person or agency to whom the disclosure was made.

f. The accounting of disclosure must be made available within 60 calendar days of the facility's receipt of the request, except for disclosures made for health oversight activities or law enforcement purposes authorized by 38 C.F.R. §1.576(b)(7) and 45 C.F.R. §164.528(a)(2)(i).

i. If the accounting cannot be provided within the specified timeframe, the timeframe may be extended 30 days.

ii. In order to extend the timeframe, the requestor must be issued a written statement from the facility Privacy Officer that includes the reasons for the delay and the date by which the accounting will be provided. Only one such extension of time for action on a request for an accounting of disclosures is permitted.

C. **Uses and Disclosures**

(1) Minimum Necessary

a. The minimum necessary requirements do not apply to disclosures to, or requests by, a health care provider who requires the information for treatment purposes.

b. All facility staff should have minimum necessary (for completion of job duties) access to PHI. Specific minimum necessary policies and procedures, including appropriate staff access levels, are explained in VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information.

c. The functional categories for each employee shall be assigned upon new hire or change in job position and reviewed annually during performance appraisals and/or annual competence assessment reviews by an employee's immediate supervisor based on VHA Handbook 1605.02, Appendix B.

i. Supervisor will advise employees of their functional category (or categories) to carry out their assigned job duties.

ii. The functional category will be annotated on the employee's performance appraisal form or proficiency report.

iii. The Employee's signature on VHA Form 10-0539, Assignment of Functional Categories) will signify their acknowledgment of the functional category, extent of access to VA information, and rules for limitations to access information on a need-to-know basis for their job duties.

iv. VHA Form 10-0539 is to be stored in Employee Competency Folder in the first tab under the performance appraisal/proficiency report.

v. The functional category selection is specifically listed by the job type for each member of the workforce on the VHA Form10-0539. If a Service Chief or designee is having difficulties determining which category a workforce member falls under they

should contact the facility ISO or PO to assist in the functional category selection.

vi. After the annual completion of all workforce member functional category forms, each Service Chief or designee shall send an email to the PO or designee attesting to the completion of all functional category forms for the employees within their department or section.

vii. During Privacy rounds the Privacy Officer will periodically ask to view a random sample of employee competency folders to check for compliance with the functional category requirements.

d. Employee access to PHI will be determined by the employee's position description and in turn, their menu access to VistA. If PHI access is granted, the employee's supervisor must determine their functional category for placement on the individual performance appraisals or proficiency reports.

(2) Authorizations

a. The facility does not use or disclose III without appropriate authority conferred by applicable federal privacy laws and regulations or individual written authorization. Valid authorizations are used only for the purpose(s) stated in the authorization and only disclosed by or released to the personnel or office listed in the authorization.

b. A written authorization signed by the individual to whom the health information or information pertains is required when:

i. The facility needs to use III for a purpose other than treatment, payment, and/or health care operations, and other legal authority does not exist; and

ii. The facility discloses information for any purpose for which other legal authority does not exist.

c. An authorization to release information must be made in writing and include the following information:

i. The identity (i.e., full name, date of birth and last four of the social security number for scanning purposes) of the individual to whom the information pertains.

ii. Veteran Request: If 38 U.S.C. §7332 protected health information is to be disclosed, this information must be specifically identified by checking the boxes.

iii. If the authorization indicates specific 38 U.S.C. §7332 protected health information is to be released to include future health information with a future expiration date but the Veteran does not have the indicated 38 U.S.C. §7332 protected diagnosis at the time of signature, the authorization is considered to be invalid for any future 38 U.S.C. §7332 protected information acquired after the signature. This newly acquired §7332 protected information cannot be disclosed without a new authorization being obtained. Marking all boxes on VA Form 10-5345 for 38 U.S.C. §7332 protected health information when the Veteran only has one is not an acceptable practice. If the Veteran marks all 38 U.S.C. §7332 boxes and does not have the diagnoses AND this authorization is for a one time use, then the authorization is still valid.

d. A description, which identifies the information in a specific and meaningful fashion, of the information to be used or disclosed.

e. The name of the person(s) or office(s) authorized to make the requested use or disclosure.

f. The name or other specific identification of the person(s) or office(s) to which the agency may make the requested use or disclosure.

g. A description of the purpose(s) for the requested use or disclosure. A statement "insurance purposes" etc., is sufficient. A purpose is not required when disclosing the information to the individual to whom the information pertains.

h. An expiration date, condition or event that relates to the individual or the purpose of the use or disclosure of the information. If the purpose section is not filled out and there is no expiration date, condition or event, the authorization is considered invalid. Examples of appropriate expiration date language specific to research are:

i. The "end of research study", or similar language, is sufficient if the authorization is for use or disclosure of III for research.

ii. The statement "none" or similar language is sufficient if the authorization is for the agency to use or disclose III for a research

database or research repository. The statement "none" cannot be used as an expiration date for any purpose other than research.

i. The signature of the individual, or someone with the authority to act on behalf of the individual, the date of the signature must be included on the authorization.

j. A statement that the individual has the right to revoke the authorization in writing except to the extent that this facility has already acted in reliance on it, and a description of how the individual may revoke the authorization.

k. A statement that VHA, this facility, or the entity requesting the information may not condition treatment, payment, enrollment, or eligibility for benefits on the individual's completion of an authorization. **NOTE**: This statement is only required if the requestor is another HIPAA covered entity.

l. A statement that III disclosed in response to the authorization may no longer be protected by federal laws or regulations and may be subject to re-disclosure by the recipient.

m. All requests for health information should be reviewed by the Release of Information Department.

n. Authorization may be given:

i. On VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information, or any subsequent authorization form approved to replace this form or a specific authorization developed for a specific VA program, e.g. eHealth Exchange, CHOICE Program.

ii. Using an outside entity's authorization form (e.g., Social Security Administration Authorization form) as long as all of the authorization content requirements are met.

o. Information will not be disclosed on the basis of an authorization form that:

i. Fails to meet all the preceding requirements;

ii. Has expired;

iii. Is known to have been revoked;

iv. Has been combined with another document to create an inappropriate compound authorization; or

v. That is known, or in the exercise of reasonable care should be known, to facility staff as false with respect to any item of the authorization requirements.

vi. The ROI Department is responsible for handling invalid authorizations. This could be by returning the invalid request form to the requestor with a letter describing the denial due to invalid authorization and including the proper VHA 3rd party Release of Information form or obtaining the authorization from the veteran or their representative. ROI is to contact the Chief of HIMS or the PO if they have questions or concerns. Chief of HIMS or designee.

vii. The ROI staff will send the requestor a missing element letter from the ROI software, DSS ROI unless 38 U.S.C. §7332 protected health information is involved.

viii. Facility staff will not check off any of the 38 U.S.C. §7332 boxes on the VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information, unless the individual is specifically asked in person while a clerk completes the form for the individual prior to signing or a telephone discussion with the individual before mailing the authorization for signature. Staff may not arbitrarily check off boxes without the individual's oral/written approval. If boxes are not checked, oral approval of sensitive information may be documented by having the ROI supervisor with a witness confirming the veteran selection by making notation on the authorization form and in the comment field in DSS ROI. The other option is the return form to veteran for correction.

(3) Processing a Request for Release of Information

a. Anyone may request VHA to disclose any record. Any request for information maintained in VHA and facility records must be processed under all applicable confidentiality statutes and regulations.

b. A request for copies of facility records must be in writing, under the signature of the requestor, and describe the record(s) sought, so it may be located in a reasonable amount of time.

c. All written requests for copies of individually identifiable health information maintained within the facility will be forwarded to the ROI Department except as indicated below. The facility Privacy Officer will be

consulted on any requests received that are unusual or are not addressed in this policy.

i. The Medical Care Cost Recovery (MCCR) Coordinator, or equivalent, is responsible for disclosing billing information. MCCR staff is also responsible for coordinating with Release of Information staff in order to account for disclosures of health information.

d. All ROI requests processed by outside of the ROI department will be submitted to Release of Information to capture the disclosures using a spreadsheet as identified in the ROI Statement of Practice.

e. The ROI Department will need to determine who is making the request for a copy of the facility record or information.

i. If the requestor is the individual to whom the records pertain, follow the guidance under B. Individuals Rights, 2.0 Right of Access.

ii. If the requestor is other than the individual to whom the record pertains (third party), determine what information or record is requested and for what purpose and is there a written valid authorization from the individual or other legal authority prior to disclosure.

f. The ROI Department will determine what information is being requested.

i. If the record requested does not contain individually identifiable information, process the request in accordance with section D. Freedom of Information Act.

ii. If the record requested contains individually identifiable information, review the paragraphs under C. Uses and Disclosures, 4.0 Uses/ Disclosures for Treatment, Payment, and Health Care Operations, and Other Operations Not Requiring Authorization for guidance directed at the specific requestor and/or purpose.

iii. If the record requested contains individually identifiable information and the guidance in section C. Uses and Disclosures, 4.0 Uses/ Disclosures for Treatment, Payment, and Health Care Operations, and Other Operations Not Requiring Authorization is not applicable and a signed, written authorization was not received, refer the request to the facility Privacy Officer for an opinion. The facility Privacy Officer will review the request and determine if

disclosure authority exists by reviewing the applicable Federal privacy laws and regulations.

iv. If the request is on a deceased individual, process the request in accordance with section C. Uses and Disclosures, 5.0 Deceased Individuals.

g. The ROI Department must process requests for individually identifiable information within specified time standards and charge the applicable fees, as appropriate.

i. Requests for copies of individually identifiable information must be answered within 20 workdays from the date of receipt.

ii. When, for good cause shown, the information cannot be provided within 20 workdays from the date the request was initially received, the requester must be informed in writing as to the reason the information cannot be provided and the anticipated date the information will be available.

iii. Copying fees may be charged for copies of records provided to requestors. Only copying fees as stated in 38 C.F.R. §1.577(f) or subsequent regulations may be charged. The facility is prohibited for charging more for copies than is allowed in VA regulations

h. A requestor may ask that the facility disclose or provide individually identifiable information in an electronic format, such as on Compact Disk (CD), in lieu of paper copies. When the records requested exist electronically and can be reproduced in the requested format, the facility must accommodate such a request. The ROI Department will work with IRM when records are requested in an electronic format. The ROI staff will follow their process for burning records on CD as required. They will also QA the information to ensure that is belongs to the correct patient before release.

(4) Uses/Disclosures for Treatment, Payment, and Health Care Operations, and Other Operations Not Requiring Authorization

a. This facility uses and discloses IIHI as permitted by the HIPAA Privacy Rule, the Privacy Act of 1974 and other federal rules and regulations. Certain disclosures, within VA, for purposes other than treatment, payment, and health care operations, may be made without authorization.

b. Individuals are not required to and cannot be forced to waive their rights under the HIPAA Privacy Rule, 45 C.F.R. §160.306 as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

c. The facility workforce (e.g. staff, employees, volunteers) uses and discloses IIHI in the following manners:

i. Within VHA on a need to know basis for treatment, payment, and/or health care operations without the written authorization of the individual.

ii. To the extent necessary, on a need-to-know basis, and in accordance with good medical and/or ethical practices, staff may disclose general patient information to the patient's next-of-kin. If the patient is listed in the facility directory, staff also may disclose to the general public, without authorization, the patient's location and general condition.

iii. To next-of-kin and family members in the presence of the individual if the patient does not object or if it is reasonably inferred from the circumstances that the patient does not object.

iv. To next-of-kin and family members when, in the professional judgment of attending medical center staff members, disclosure is in the best interest of the patient.

v. To VBA for use in the determination of eligibility for, or entitlement to, benefits.

vi. To VA contractors or business associates for a contracted service or service provided on behalf of the facility related to treatment, payment, and/or health care operations provided that the disclosure is within the scope of the contract or agreement and when necessary, a signed BAA with the contracted company or business associate is on file.

vii. To a receiving facility when a patient is transferred to, or being treated at a community hospital (including other federal hospitals), State Veteran Home, or community nursing homes.

viii. To the Office of Resolution Management (ORM) when necessary for determining compliance with Equal Employment Opportunity (EEO) requirements and upon the request of the Office of Resolution Management.

ix. To the Board of Veterans Appeals for benefits, including the processing and adjudication of claims appeals.

x. To the National Cemetery Administration for determinations of eligibility for, or entitlement to, benefits.

xi. To VA Unions, in the course of fulfilling their representational responsibilities. VA Unions may make a request to management for copies of facility records pursuant to its authority under 5 U.S.C. § 7114(b) (4). Unions may request any records that are maintained by a VA facility. For example, this might include releasable portions of completed Administrative Investigation Boards (AIB), patient medical records and/or an employee's personnel records. However, under certain circumstances, unions may not be legally entitled to receive IIHI, or information protected by other statutes such as the Privacy Act. All requests for information submitted by VA Union Representatives are referred to the servicing HRMS, which coordinates the response with the Regional Counsel and the facility Privacy Officer (designee) and/or the facility FOIA Officer (designee).

xii. To a Member of Congress (including a staff member acting on the Member's behalf) when responding to an inquiry from a Congressional office that is made at the request of the individual to whom the information pertains under the following conditions: (check the fact sheet that is posted)

1) If prior written authorization has not been provided and the Member provides a copy of the original correspondence from the individual requesting the member's assistance.

2) If a prior written authorization is provided and conforms to the requirements of a valid authorization.

3) If the request is not the result of an inquiry made on behalf of the individual's family or another third party. VAMC staff cannot provide information to a Congressional member if the inquiry was initiated by a family member or person other than the individual to whom the information pertains.

4) To a Member of Congress (including a staff member acting on the Member's behalf) when responding to an inquiry from a Congressional office that is made at

the request of the individual to whom the information pertains under the following conditions:

a) If prior written authorization has not been provided and the Member provides a copy of the original correspondence from the individual requesting the member's assistance.

b) If a prior written authorization is provided and conforms to the requirements of a valid authorization.

c) If the request is not the result of an inquiry made on behalf of the individual's family or another third party. VAMC staff cannot provide information to a Congressional member if the inquiry was initiated by a family member or person other than the individual to whom the information pertains.

d) The Medical Center Director has designated the Public Affairs Officer (PAO) as the spokesperson for this Medical Center and the Community Based Outpatient Clinics (CBOC's) in all contacts with the offices of elected officials. Official inquiries, information requests, meeting requests, and all forms of contact received or initiated at this Medical Center or the CBOC's which concern VA in general or this Medical Center and its programs, policies, and functions, should be referred to the PAO immediately upon having contact with the office of the elected official. The PAO may seek information for response to inquiries from elected officials from various Medical Center resource employees, or may request that such employees directly respond to an inquiry.

e) Any response to the office of an elected official by any employee or staff member that has not been approved by the Medical Center Director or designee will be considered the representation of a private citizen and not that of this Medical Center or VA. Individuals who choose to respond to or who initiate contact with elected officials outside of this policy accept full responsibility for their statements. They are not authorized to do so while

on duty status and are not authorized to use VA equipment (including telephones or computers) or stationery in such contacts, unless doing so as directed by the PAO or Medical Center Director.

f) To health insurance carriers or health plans for payment activities related to seeking reimbursement for VA care.

g) To General Counsel and/or Regional Counsel for the purposes of health care operations, e.g. legal services, as long as a business associate agreement is in effect. In addition, information may be provided to the Office of General Counsel (OGC) for any official purpose authorized by law as long as VHA Central Office maintains a MOU or BAA with OGC authorizing the sharing of IIHI for legal counsel provided to VHA.

h) Except for criminal law enforcement activities, to the VA Inspector General or Office of Inspector General (OIG) Investigators for any official purpose authorized by law, such as health care oversight.

i) Except for criminal law enforcement activities, to the facility VA Police for enforcement of physical security (e.g., escort of high-risk patients).

j) To the VA Office of Employment Discrimination, Complaints, and Adjudication (OEDCA) to review the merits of employment discrimination claims filed by present and former VA employees and non-agency applicants for employment.

k) To the VHA Office of Medical Inspector (OMI) to address health care problems to monitor and improve the quality of care provided by VHA.

l) To the United States Office of Special Counsel (OSC). The U.S. Office of Special Counsel (OSC) is an independent agency that enforces Whistleblower protections, safeguards the merit

system and provides a secure channel for whistle blower disclosures.

m) VA Human Resources Management Services (HRMS). VHA may disclose individually-identifiable information to VA HRMS as authorized by law. There is no authority under the HIPAA Privacy Rule for the disclosure of a VA employee Veterans' health record to management or personnel officials for disciplinary investigation purposes without prior signed, written authorization from the employee.

d. VA Researchers.

i. VHA may use employee information, including health information for official VHA research studies, in accordance with VHA Directive 1200, Veterans Health Administration Research and Development Program, other applicable 1200 handbook series, and 38 CFR Part 16.

ii. For use or disclosure of individually-identifiable health information involving non-employee research subjects for research purposes (see paragraph 13, Research).

iii. If the research involves pictures or voice recordings for other than treatment purposes, the Informed Consent (10-0086) must state that a photograph, image or video/audio recording is going to be made. If the documentation of ICF is waived, the script for the audio-recording must include the subject's permission to be recorded.

NOTE: Use of a patient's photograph or voice for purposes other than the identification, diagnosis, or treatment of the patient is not permitted unless a signed consent is obtained on VA Form 10-3203, Consent for Production and use of Verbal or Written Statements, Photographs, Digital Images, and/or Video or Audio Recordings by VA (38 C.F.R. §1.218). If photographs are taken to support treatment, those photographs are included in the health record maintained for each patient and do not require VAF 10-3203. Disclosure of the patient's photograph or voice would require written authorization on VAF 10-5345 from the individual or personal representative. (See VHA Directive 1078(1), Privacy of Persons Regarding Photography, Digital Images and Video or Audio Recording).

e. Other disclosures are handled by ROI, Chief of HIMS, FOIA Officer, or the Privacy Officer to determine what other privacy regulations may apply. The Centralized Billing Office (CPAC) will also submit

monthly reports of accounting of disclosures used for billing purposes to the Chief of HIMS.

(5) Deceased Individuals

a. Except for uses and disclosures for research purposes discussed in section C. Uses and Disclosures, 10.0 Research Activities; this facility shall protect the PHI of a deceased individual in the same manner, and to the same extent, as required for the PHI of living individuals.

b. PHI, excluding 38 U.S.C. §7332 protected health information, of a deceased individual may be disclosed to coroners, medical examiners, and funeral directors. Title 38 U.S.C. §7332 protected health information may be disclosed for determining cause of death or required for collection of death or vital statistics per State law.

c. Disclosure of autopsy findings:

i. The Diagnostic Service Line Manager is responsible for preparing the autopsy provisional diagnoses report and ensuring its availability to the attending physician; for disclosing pathology/tissue slides/blocks; for releasing radiographic films and for following up to ensure return of this VA property and coordinating with Release of Information to account for the disclosure.

ii. Managers of Clinical Service Lines are responsible for translating autopsy findings into layman's terms and composing a timely autopsy letter in lay terminology upon request.

iii. A copy of the autopsy clinical finding summary and the listing of clinical-pathological diagnoses on Standard Form (SF) 503, Medical Record-Autopsy Protocol, are disclosed, when requested by the next-of-kin.

iv. All cases in which the autopsy reveals drug abuse, alcoholism or alcohol abuse, HIV infection, or sickle cell anemia information (which is subject to additional disclosure restrictions), the autopsy results are not disclosed to the next-of-kin unless the facility Privacy Officer has determined that such disclosure is necessary for the survivor to receive benefits.

(6) Contracts and Business Associate Agreements

a. In contracts/agreements that involve the use or disclosure of PHI, appropriate privacy requirements, specifications, and statements of work

must state that privacy requirements and specifications should be properly implemented before the contract/agreement goes into operation.

b. All contracts must meet the contracting requirements dictated by VA's Office of Acquisition and Material Management and the Federal Acquisitions Regulations (FAR). Any contract which necessitates the use of III must conform to the policies and procedures in FAR Subpart 24.1, Protection of Individual Privacy and VA Directive 6500.6, Contract Security.

c. The contracting officer, the Privacy Officer, and the ISO will work together to identify those entities that qualify as Business Associates under HIPAA and ensure that BAAs are enacted for these identified entities in accordance with HIPAA and BAA policies and procedures (NOTE: a business associate relationship exists if the facility is required to release PHI to a contractor or business partner for the provision of services on the facility's behalf.)

d. All contracts, agreements, and relationships must be assessed to determine if a business associate relationship exists.

e. If a business associate relationship is determined to exist, a business associate agreement is enacted utilizing only the most current version of the VHA Health Information Access Office approved BAA language available at http://vaww.vhadataportal.med.va.gov/PolicyAgreements/BusinessAssociateAgreements.aspx.

f. If a business associate is determined to serve more than one VA facility, the facility Privacy Officer should contact the VHA Health Information Access (hia.va.gov) mail group to discuss enacting a national BAA. Any national BAA takes precedence over a local BAA. Local and regional BAAs should not be initiated if a national BAA exists for the same services as described in the national BAA preamble. BAAs are kept updated and documented as long as the agreement is in force. (Refer to VHA Handbook 1605.05, Business Associate Agreements)

g. Per the agreement, business associates will abide by the terms and conditions spelled out in the agreement.

h. If a pattern of activity or practice of the business associate constitutes a material breach or violation of the business associate's obligation under the contract or other agreement is discovered, the facility Privacy Officer reports the problem to NSOC and works with the Contracting Officer for resolution. All Business Associates must report

the breach within 24 hours to the Director of Health Information Governance and submit a written report within 10 days.

i. The Contracting Officer's Representative (COR) responsible for the contract will monitor compliance with the applicable privacy policies required under the Business Associate Agreement with assistance and in consultation with the facility Privacy Officer.

(7) Emergency Situations and Serious/Imminent Threats

a. When an employee becomes aware of a threat to the patient, another individual (e.g. family of veteran) or to the public, the VAMC staff should contact the facility Privacy Officer in order to determine if, and how, to report or address the serious and imminent threat to the health or safety of the patient, other individual or public.

b. CMCVAMC employees to include the Privacy Officer will follow Medical Center Memorandum No. 07B-06 when handling or responding to threats

c. When a local law enforcement agency approaches CMCVAMC staff to obtain health information on a Veteran or patient due to a current or ongoing serious and imminent threat to the public, the facility Privacy Officer and VA Police should be contacted. During regular business hours, the facility Privacy Officer will make the disclosure of requested health information to the law enforcement officials in a position to prevent or lessen the threat. Such disclosure should be made immediately once the facility is made aware of the serious and imminent threat. If health information is needed after hours, the AOD should be contacted by VA Police to assist local law enforcement officials in obtaining information to lessen or prevent the threat.

d. VHA may disclose IIHI, excluding 38 U.S.C. §7332-protected health information, in accordance with:

i. 5 U.S.C. §552a(b)(8)- to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if, upon such disclosure, notification is transmitted to the last known address of the individual to whom the records pertain; and

ii. 45 C.F.R.§ 164.512(j)(1)(i)- to avert a serious and imminent threat to the safety of an individual as long as the disclosure is made to a party which is in a position to prevent or lessen the threat, such as a law enforcement official or the individual threatened; or

iii. 45 C.F.R. § 164.512(k)(2)- to avert serious threats to the safety of the public as long as the PHI is given to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, or other national security activities.

NOTE: This disclosure requires an accounting of disclosure through the ROI Plus software. Also, a notification letter must be sent to the person to whom the health information pertains. The person has a right to know who received their information and what information was disclosed by VHA.

(8) Standing Letters

a. VHA may disclose IIHI, excluding 38 U.S.C. 7332 protected information, pursuant to a valid standing written request letter to State Agencies charged with the protection of the safety and health of the public. Information disclosed in response to a standing written request letter is provided for the purpose of cooperating with a State law enforcement reporting requirement. Regional Counsel will be consulted to determine if State laws would allow for standing written request letter to be implemented.

b. Standing written request letters may be needed for the following purposes:

i. Law Enforcement- Law enforcement entities routinely require reporting from VHA records for suspected child abuse, suspected elder abuse, gunshot wounds, and other administrative actions, e.g., suspension or revocation of a driver's license.

ii. Public Health- Examples of public health reporting requiring a standing written request letter include:

a) Communicable diseases (e.g., hepatitis, tuberculosis, sexually transmitted diseases, etc.);

b) Vital statistics (e.g., deaths, etc.); and

c) Other State reporting requirements (e.g., animal bites).

iii. State and Other Public Registries (e.g. State Cancer Registries, NOTE: VHA may not disclose individually-identifiable information to private registries without the prior

written authorization of the individual to whom the information pertains.)

iv. Coroner or Medical Examiner

c. With the exception of public health reporting requirement defined in VHA Directive 2013-008, Infectious Disease Reporting, all other disclosures are discretionary on behalf of the facility.

d. The facility Privacy Officer is responsible for ensuring all standing written request letters meet the guidelines as defined in 1605.01 (21)b. A copy of all standing written request letters must be maintained by the facility Privacy Officer and renewed every 3 years.

e. The Privacy Officer is responsible for obtaining, maintaining and renewal of all valid standing written request letters on file. The Privacy Officer will solicit from Service Chiefs, the State agencies where routine disclosure are made based on State law. A SharePoint site with routine standing written request letters will be placed on a facility shared drive for access by AODs, Infection Control staff, Social Workers, VA Police, Laboratory, Chief HIM, etc.

f. Departments responsible for disclosing information pursuant to a valid standing written request letter must coordinate the disclosure with the Release of Information Department or Privacy Officer in order to account for the disclosure.

g. If a standing letter is not in place the party requesting the IIHI must submit a written request under the authority of 5 U.S.C. 552a(b)(7) for the information. The request must be:

i. In writing.

ii. Specify the particular portion of the record desired.

iii. Specify the law enforcement activity or purpose for which the record is sought.

iv. State that de-identified data could not reasonably be used.

v. Be signed by the head of the agency.

(9) State Prescription Drug Monitoring Program

a. VHA may disclose individually-identifiable health information to a State Prescription Drug Monitoring Program (SPDMP) without the signed, written authorization of the Veteran for whom the medication was prescribed. Disclosure may be for the purpose of querying the SPDMP or

reporting mandatory prescription information to the State (e.g., batch reporting).

NOTE: Batch reporting is currently available. Please work with your local IT and Pharmacy departments to ensure appropriate use and functionality of the process.

i. The Chief, Pharmacy Service tracking the accounting of disclosures when querying the SPDMP.

ii. A note in CPRS can be used to account for the SPDMP query disclosures; however, the Chief of HIM should be involved in the development of the note template.

(10) De-identification of PHI

a. Information is only considered de-identified if the methods outlined in VHA Handbook 1605.01 are followed. Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual **and** if VHA has no reasonable basis to believe it can be used to identify an individual. This is accomplished by either

i. having an expert with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and documents the methods and results of the analysis that justify such determination; or

ii. all eighteen (18) identifiers listed in VHA Handbook 1605.01 are removed.

b. De-identified data is not PHI. Therefore, when data is appropriately de-identified, the HIPAA Privacy Rule, the Privacy Act and other federal privacy regulations do not apply and information may be disclosed under the Freedom of Information Act.

c. VA Directive 6511 Presentations Displaying Personally Identifiable Information must be followed prior to presenting at VA and non-VA conferences. Any questions concerning whether or not information is de-identified prior to disclosure, should be referred to the facility Privacy Officer.

(11) Research Activities: General

a. VA Research investigators must have appropriate legal authority to collect, access, or use individually identifiable information in a research study. The "need-to-know" in their official performance of their job duty does not cover all federal privacy regulations specific to research.

NOTE: The facility Privacy Officer and the facility Information Security Officer will serve in non-voting capacities on the Institutional Review Board (IRB) pursuant to VHA Handbook 1200.05 Requirements for the Protection of Human Subjects in Research.

b. The facility Privacy Officer will review all initial submissions of human subject research protocols, including exempt protocol submissions, for the use and/or disclosure of individually identifiable information and other privacy considerations prior to the convened Institutional Review Board Meeting (IRB) at which the study is to be reviewed, except for those research projects approved by the VA Central IRB. It is expected that review submissions and approval process will be timely submitted by all parties involved. The Information Security Officer will review all initial submissions of human subject research protocols for compliance with all applicable federal security requirements. The Privacy Officer and the Information Security Officer will provide a final written summary to the IRB. The Privacy Officer's final written summary must include approval of the HIPAA Authorization and validation that the IRB appropriately approved the waiver of HIPAA Authorization as appropriate prior to the use and/or disclosure of III by the researcher or his/her team.

c. The facility Privacy Officer and Information Security Officer will review all continuing reviews of human subject protocols or proposed human subject protocol amendments impacting privacy or information security. All IRB protocols and amendments impacting privacy or information security is placed on the IRB SharePoint Site. The Privacy Officer and Information Security Officer are included in an email sent from the IRB Program Specialist indicating the documents are ready for review. The Privacy Officer and Information Security Officer will document stipulations found in the protocol and request clarification from the Principle Investigator. The stipulations are listed in the IRB minutes. When the stipulations have been they are listed in the minutes as "stipulations met continuing review or stipulation met amendment. Once the stipulations are met, the Privacy Officer and Information Security Officer are required to sign off on the protocol as final review.

d. Facility research office staff verifies the qualifications of VA researchers seeking to use and/or disclose III, (i.e. they have completed

their mandatory privacy and security training) and ensures that the VA researchers take appropriate measures to protect the privacy of study subjects.

(12) Research Activities: Use

a. VA Research investigators may use III for reviews preparatory to VA research, provided that the information is being sought solely for purposes preparatory to research and that no PHI will be removed by the VA researcher. All other requirements related to the use of III for reviews preparatory to VA research are set forth in VHA Handbook 1200.05; Requirements for Protection of Human Subjects Research must be followed.

b. VA Research investigators may use PHI for VA-approved research if the facility Privacy Officer has determined that:

i. A Research HIPAA authorization compliant with VHA Handbook 1605.01 Para. 14 will be obtained for each research subject; or

ii. The IRB has approved a waiver of HIPAA authorization, in full or in part, and the IRB approval has been appropriately documented as required by the HIPAA Privacy Rule and VHA Handbook 1200.05; or

iii. A Limited Data Set will be used and a valid DUA has been signed as required by the HIPAA Privacy Rule.

c. If the researcher has not completed his or her study by the time of the expiration of the Research HIPAA authorization, the researcher can no longer use any of the information previously collected from the study subjects.

d. PHI/III and other VA sensitive data for a VA-approved research study that is stored, collected, or maintained outside of VA custody, either electronic or paper must have prior approval and safeguards in place to protect the data. The facility Privacy Officer will work with the facility Information Security Officer and Chief Information Officer to ensure the appropriate safeguards are in place. See VA Handbook 6500 for further guidance.

e. For certain sensitive research studies, a VA researcher may request a Certificate of Confidentiality from the National Institutes of Health (NIH) which, if granted could prevent the facility from being forced to disclose individually identifiable information on research subjects, by a

court order/subpoena in any civil, criminal, administrative, legislative, or other proceedings that are maintained in 34VA12, Veteran, Patient, Employee, and Volunteer Research and Development Project Records.

(13) Research Activities: Disclosure

a. For the facility to disclose protected health information to a non-VA researcher or other non-VA entity for research purposes, either for VA research purposes, or for non-VA research programs , there must be legal authority under all applicable federal privacy laws and regulations including 38 U.S.C. § 5701, the Privacy Act, HIPAA Privacy Rule and 38 U.S.C. §7332. The applicable legal authority is as follows:

i. 38 U.S.C.§ 5702 – If the non-VA researcher or non-VA entity is requesting III, that may be disclosed under 38 U.S.C. § 5701, a written request stating records sought and purpose of the records that is dated and signed by the non-VA researcher is required. If VA is initiating the disclosure of information under 38 U.S.C. § 5701 for a research purpose, a written request from the non-VA researcher or non-VA entity is not required.

ii. 38 U.S.C. § 5701 – For purposes of disclosing records pertaining to any claim under any of the laws administrated by the Secretary for non-VA Research , a "federal" non-VA researcher may be provided name and address of individuals under 38 U.S.C. § 5701(b)(3). For a "non-federal" researcher or other entity, the researcher or entity must provide to VA the names and addresses of the individual whose claims information is being sought in order to obtain those individuals' identifiable information.

iii. 38 U.S.C. §7332 – The non-VA researcher to whom 38 U.S.C. §7332 protected health information (related to drug abuse, alcoholism, or alcohol abuse, infection with the human immunodeficiency virus, or sickle cell anemia) is disclosed must provide written assurance that the purpose of the data is to conduct scientific research and that no personnel involved in the study may identify, directly or indirectly, an individual patient or subject in any report of such research or otherwise disclose patient or subject identities in any manner. This assurance may be documented in the research protocol. In addition, the Medical Center Director based on input from the ACOS, Research and Development must determine that the non-VA researcher is qualified to conduct the research; has a research protocol that stipulates how the information will be maintained in a secure manner; and a written statement that the research protocol has been reviewed by an IRB who found that the individual's rights are adequately protected and

that the potential benefits of the research outweigh any potential risks to patient confidentiality.

NOTE: If a VA researcher plans to disclose 38 U.S.C. §7332 protected health information to an outside non-VA entity or use within a publication, this written assurance must also be obtained.

iv. Privacy Act of 1974 – If an individual does not provide prior written consent for the disclosure of his/her record contained in a system of records (SOR), there must be a routine use under the applicable Privacy Act System of Records that permits the disclosure. (See 34VA12, Routine Use 19)

v. HIPAA Privacy Rule – Either a research HIPAA authorization compliant with VHA Handbook 1605.01 Para. 14 will be obtained for each research subject; or the IRB has approved a waiver of HIPAA authorization and the IRB approval has been appropriately documented as required by the HIPAA Privacy Rule and VHA Handbook 1200.05.

NOTE: A waiver of HIPAA authorization approved by the IRB does not affect or override the other legal requirements that must be met.

b. A VA researcher must have appropriate legal authority to disclose individually identifiable information to a non-VA entity, including a research sponsor or an academic affiliate who is collaborating on this study. This disclosure authority is outlined in the written HIPAA authorization signed by the individual unless other legal authority exists, e.g., Court Order.

c. Decedents' information may be disclosed to a source other than the researcher who has use of this data if the HIPAA Privacy Rule allows for disclosure to a non-VA entity. See your facility Privacy Officer in regards to any questions concerning disclosure authority.

d. This facility may distribute a limited data set, information that excludes direct identifiers, but still contains potentially identifying information, without consent of the individual. A limited data set is only protected under the HIPAA Privacy Rule as the data is not considered identifiable for purposes of the Privacy Act and 38 U.S.C. §7332. Disclosure of a limited data set is dependent upon the receipt of a DUA, which must:

i. Establish the permitted uses and disclosures of the information;

ii. Establish who is permitted to use or receive the data set; and

iii. Provide that the data set recipient:

1) Does not use for further disclose the information other than as permitted.

2) Uses appropriate safeguards to prevent improper use or disclosure of the information;

3) Reports to the facility/VHA any improper use or disclosure of which it becomes aware.

4) Ensures that any agents to whom it provides the data set agrees to the same restrictions and conditions that apply to the data set recipient.

5) Does not identify the information or contact the individuals.

e. A contracted entity involved in VA research is not a business associate of the covered entity and no business associate agreement is required.

f. A research disclosure made pursuant to a signed, written research HIPAA authorization to a non-VA entity (study monitor, sponsor, academic affiliate, or other non-VA entities) who is not a research team member or contractor requires an accounting of disclosure to be maintained. The accounting of disclosure may be maintained concurrently or be created retrospectively from the VA researcher's files. See above Section B, Individual's Rights, 8.0 Accounting of Disclosures.

g. Facility will not disclose any personal information about VHA personnel engaged in animal research in response to a FOIA request if the FOIA Officer determines a risk to the facility or research personnel.

NOTE: Further guidance on Research requirements is available in VHA Handbook 1605.01, VHA Handbook 1081.01 Data Use Agreements, VHA Directive 1200, and other applicable 1200 series handbooks.

(14) Logbooks

a. Unnecessary collection of sensitive personal information (SPI) in physical logbooks is prohibited.

b. Logbooks containing sensitive personal information must only be maintained for a VHA compelling business need. Use of an unapproved physical logbook will be considered a privacy violation. An approved physical logbook may only contain those data elements that are necessary to satisfy the compelling business need. Individuals are prohibited from compiling historical documentation containing SPI that is not directly related to an approved compelling business need.

c. VHA SPI contained in approved physical logbooks must be handled and maintained in a secure manner with measures in place to prevent the unauthorized disclosure of SPI data. The physical logbook shall be treated as "For Official Use Only" and shall not be removed from its intended place of business except to securely store it.

d. Procedures:

i. Use of a Logbook by an Individual. Any instance of an individual maintaining a physical logbook which contains or refers to VA sensitive information will be considered a breach of security unless use of the logbook has been expressly approved by the Director. VA employees are prohibited from compiling historical documentation containing SPI which is not directly related to an approved business requirement. Any instance of a VA employee maintaining a physical logbook for personal use that contains or refers to patient or employee SPI, will be considered a privacy violation.

ii. Electronic Logbooks. When a CMCVAMC service, affiliated organization, or office (including the medical center and outpatient clinics) identifies a compelling, existing business need for a physical logbook containing SPI, the VA employee must work with the appropriate Privacy Officer (PO) and/or Information Security Officer (ISO) to identify an alternative to a physical logbook. Alternatives may include securing the information on secure network drives.

iii. Physical Logbook Inventory and Approval. When no other alternatives can be achieved, physical logbooks must be approved by the Director in accordance with the PVAMC policy and approval process. Waiver/exception requests must be submitted in writing to the Director (using Attachment A). These requests must describe efforts made to create an electronic alternative and why such an alternative is not feasible. Service chiefs must attest to the business requirement, location, security controls, and content by completing Attachment A and submitting it to the Privacy Officer.

iv. If a written/physical logbook is approved, it must include the least information possible to perform its purpose. A full Social Security Number, claim number, date of birth, or other unique identifier should not be used unless necessary as described in a VA Directive or federal regulations.

v. The service chief must document appropriate security measures to prevent the loss of the physical logbook and/or log pages. At no time will a physical logbook be left unattended in a public area; logbooks must be physically secured when not in use and at the end of business day.

vi. Director Approval Not Required. Only when a written/physical logbook is used to facilitate daily entries and destroyed daily. For example, an office having a small staff may use a physical logbook to track visitors or patients; however, at the end of the day the data must be transferred to an electronic tracking system or log and the physical logbook pages must be shredded using a VA approved method.

vii. When a staff member or Service needs a physical logbook containing SPI to meet or satisfy a compelling business need or requirement, the facility program or service requesting the physical logbook will work with PO to evaluate if a physical logbook is required. When no other alternative can be achieved, physical logbooks may be approved by the Facility Director.

viii. Supervisors, service chiefs or other responsible parties will attest to the compelling business requirement (why it is needed), the physical location (where the physical log book will be kept both during and after normal business hours), the extent of security controls (how the logbook will be protected), and a list of the elements that are being collected in the physical logbook.

ix. When a staff member or Service needs a physical logbook containing SPI to meet or satisfy a compelling business need or requirement, the facility program or service requesting the physical logbook will work with PO to evaluate if a physical logbook is required. When no other alternative can be achieved, physical logbooks may be approved by the Facility Director.

x. If a compelling business need is identified and alternative to a physical logbook has not been identified then the VHA facility must work with the appropriate PO, ISO, and RM to make the logbook electronic and secure within VHA technical systems with appropriate information technology (IT) security controls. Every

effort will be made to furnish equipment (such as encrypted thumb drives) or technology (secure shared drives) that will meet the compelling business need in an alternate secure fashion. The solution provided to the staff member, service or program must adequately address the identified business need.

xi. Approved physical logbooks must be maintained no longer than their useful purposes and in accordance with VHA Records Control Schedule 10-1.

xii. Exceptions: Notwithstanding the above, a physical logbook is authorized in the following instances:

1) Emergency or computer contingency plan physical log book used in a national disaster or when computers are down.

2) Facility Sign-in Roster. A sign-in roster is a temporary record that may be maintained for the purpose of personnel accountability such as training; or management of appointment scheduling. Sign-in rosters shall contain only the name and the time/date of access or arrival and purpose for visit (when in a non-clinical environment). Sign-in rosters will remain in direct unobstructed view of VHA staff. Sign-in rosters used for the purpose of appointment check-in shall contain only the name or signature and the time/date of access or arrival and must be destroyed at the completion of each business day using a VHA- approved destruction method. In clinical settings, supervisors shall implement measures to prevent patients from viewing the names and other SPI of patients who have previously signed in.

3) VHA Form 4793, Visitor Register. Visitor registers may be used to record the name, destination, check in and checkout times of individuals when they are visiting an area. Registers may be placed, as necessary, at several locations throughout a facility. At the end of the day the data must be destroyed or if there is a requirement to keep the data for a longer period of time the data must be transferred to an electronic tracking system or log, and the physical logbook pages must be shredded using a VHA approved method.

4) Security monitoring of restricted areas such as computer rooms. A sign in sheet in a computer room may

be maintained for the purpose of personnel accountability. If there is a requirement to keep the data for longer than a day then all security and NARA requirements must be met.

xiii. Exceptions: Notwithstanding the above, a physical logbook is authorized in the following instances:

D. **Freedom of Information Act (FOIA)**

(1) General

a. The FOIA, Title 5 United States Code (U.S.C.) 552, implemented by Title 38 Code of Federal Regulations (CFR), Sections 1.550-1.562 provides that any person has the right to obtain access to federal agency records, except to the extent that such records or portions of them are protected from public disclosure by one of the nine FOIA exemptions or by one of three special law enforcement record exclusions.

b. The FOIA requires disclosure of reasonably described VA records, or a reasonably segregable portion of the records, to any person upon written request, unless one or more of the nine exemptions apply to the records.

c. A FOIA request may be made by any person (including foreign citizens), partnerships, corporations, associations, and foreign, State, or local governments with some exceptions. The following types of request are not proper FOIA requests:

i. Requests for records by Federal agencies and their employees acting in their official capacity.

ii. Requests for records by fugitives from justice seeking records related to their fugitive status.

d. VHA administrative records not retrieved by name, social security number, or other identifier must be made available to the greatest extent possible in keeping with the spirit and intent of the FOIA.

e. Before releasing records in response to a FOIA request, the records must be reviewed by the facility FOIA Officer to determine if all or only portions of the records can be released. Portions that cannot be released will be redacted in accordance with the nine exemptions provided in the FOIA. The process of deleting portions of documents before releasing them is referred to as "redaction."

f. The FOIA mandates that all FOIA requests, absent unusual or exceptional circumstances, be processed within 20 business days of receipt.

i. To foster ongoing communication and awareness on matters of significant importance to VA and VHA leadership, the facility FOIA Officer must provide notification of substantial interest FOIA requests. A substantial interest FOIA Request is a request for information in which there has been or is likely to generate substantial public interest. This would include, but is not limited to, the following types of requests, regardless of the requester: (1) those related to a threat to the public health; (2) high profile local or national incidents or situations involving VA beneficiaries, employees or officials; and (3) incidents involving an alleged breach of the public trust (e.g., waste, fraud or abuse). If the request is from the news media, a member of Congress, or an attorney/law firm involving Agency litigation, a Sensitive FOIA Notification must be prepared and emailed to the Facility Executive Leadership Team (QUAD) as well as VHA FOIA issues mail group in the Global Address Listing (GAL). The facility FOIA Officer will notify the VHA FOIA Office of all substantial interest FOIA requests following the current procedure set forth by the VHA FOIA Office.

(2) Requests for Copies of Records

a. Records or information customarily furnished to the public in the regular course of the performance of official duties (e.g., information posted on VAMC Internet site) may be furnished without a written request. If the information sought is available on a VA or VHA public website, a CMCVAMC employee may provide the website address to the requester to avoid having the individual submit a FOIA request for the records.

b. Requests from individuals for information about themselves, which is retrieved by their names or other personal identifiers, are to be processed as outlined in section B. Individual's Rights, 2.0 Right of Access, unless the Privacy Act system of records maintaining the requested records has been exempted from a first party right of access. First party requests for records from such exempted Privacy Act systems of records will be processed under the FOIA.

c. A FOIA request may be submitted through any mail service, by facsimile or electronically to an official FOIA mailbox established for the purpose of the receiving FOIA requests. Requests for CMCVAMC records may be submitted to the facility's electronic FOIA mailbox at

vhaphifoiaoffice@va.gov or faxed to (215)823-6007 or mailed to CMCVAMC Attention: FOIA 3900 Woodland Avenue, Mail Stop 00, Philadelphia, PA 19104.

d. Requests for VHA records processed under the FOIA must be in writing and describe the records in enough detail so that they may be located with a reasonable amount of effort. If a request, regardless of the method in which the request was received (i.e., mail, facsimile or e-mail), concerns documents involving a personal privacy interest or are protected by another confidentiality statute, the request must contain an image of the requester's handwritten signature. This procedure cannot be waived for reasons of public interest, simplicity, or speed.

e. The request does not have to be designated a FOIA request in order for the request to be processed as a FOIA request and the individual seeking the documents does not have to explain why access to agency records is desired.

(3) Processing a FOIA Request

a. Any CMCVAMC employee receiving a written request for records must be promptly forwarded to the request to the facility's FOIA Officer for action. Deceased medical record requests will be received by the Release of Information department and forwarded the FOIA for review and approval. The FOIA officer will log all deceased record requests and create the final decision letter (AID).

b. Immediately upon receipt of a FOIA request, the facility FOIA Officer will date stamp the request and log request into FOIA software.

c. All FOIA requests will be entered into the Department of Veterans Affairs' electronic FOIA tracking system.

d. The facility FOIA Officer will review the request to determine if the request is made in compliance with the FOIA and VA's regulations implementing the FOIA, if the requester is seeking a fee waiver or expedited processing, if the request meets the definition of a substantial interest FOIA request, and if the request was sent to the correct agency component.

e. FOIA requests not submitted to the correct agency component will be promptly referred by the facility FOIA Officer to the correct component for processing.

f. The facility FOIA Officer will address requests for fee waivers and expedited processing in accordance with the FOIA.

g. Substantial interest FOIA request notifications will be completed in accordance local and national procedures.

h. The facility FOIA Officer shall charge for processing requests under the FOIA in accordance with the FOIA and the VA implementing regulations.

i. Within ten business days of receipt of the FOIA request, the facility FOIA Officer will acknowledge receipt of the request by sending the FOIA requester an acknowledgement letter.

i. The acknowledgment letters to the FOIA requestor will contain the following information:

1) The date of the request.

2) The date the FOIA Officer received the FOIA request

3) A description of the records sought.

4) The processing track type, e.g. simple, complex, or expedited.

5) The cut-off date of the records search.

6) The assigned FOIA request tracking number.

7) The name and contact information of the CMCVAMC FOIA Officer handling the request.

j. A reasonable search for records responsive to the FOIA request will be conducted by the CMCVAMC employees. All records responsive to a FOIA request will be forwarded to the facility's FOIA Officer for processing.

k. In instances where the FOIA requester fails to provide enough information to locate the requested records, the FOIA Officer will seek clarification from the FOIA requester.

l. In unusual circumstances, the facility FOIA Officer may extend the 20-business day time limit to process FOIA request an extra 10 business days. The FOIA Officer will notify the requester of the unusual circumstances, that a time extension has been taken, and the date which a response is expected to be issued. If the extension is more than 10

business days, the FOIA Officer will inform the requester of this in writing and provide the requester an opportunity to narrow the scope of the request or arrange for an alternate timeframe.

m. The facility FOIA Officer will respond to FOIA requestors' inquiries and questions in a timely way and keep the requestor informed during delays in processing.

n. After making a release determination, the facility FOIA Officer will issue an initial agency decision (IAD) to the requester. The IAD must contain the following information:

i. the date of the request

ii. the date the FOIA Officer received the request,

iii. the description of the records sought,

iv. the assigned FOIA request tracking number ,

v. the procedural history of the request

vi. the cut-off date of the record search

vii. the exemption(s) cited when information is being redacted or withheld and

viii. the type of information being redacted or withheld (i.e. name, SSN, address, etc.), and,

ix. if any adverse determinations are made, the right to appeal to the Office of General Counsel (OGC).

o. IADs for FOIA requests denied in whole or part must be signed by the Medical Center Director or the FOIA officer delegated under authority by the director.

p. FOIA administrative case files will be maintained in accordance with RCS 10-1 and the National Archives and Records Administration (NARA) General Records Schedule and contain the following information:

i. copy of the FOIA request,

ii. evidence demonstrating that the FOIA Officer conducted a thorough search for responsive records,

iii. un-redacted copies of responsive records,

iv. redacted copies of responsive records sent to the FOIA requestor, and

v. Copies of all correspondence, including the signed IAD letter, and contact with requesters and in the case of exemption 4, the submitter, to include, but not limited to emails and letters concerning acknowledgement, fees, scope, clarification, pre-disclosure notification, notice of intent and the initial agency decision.

NOTE: Refer to VHA Handbook 1605.01 Privacy and Release of Information paragraph 32, and Freedom of Information Act for additional information on processing FOIA requests.

(4) Coordination with Regional Counsel and VHA FOIA Officer

a. The facility FOIA Officer will consult with Regional Counsel, VISN, and the VHA FOIA Office concerning FOIA legal requirements and the handling of specific FOIA requests.

b. In any case where a FOIA request involves matters or subjects involved in ongoing or anticipated litigation, administrative proceedings, or criminal or civil investigation, health care facility personnel must coordinate the facility's response to the FOIA request with their Regional Counsel, ***James Sinwell, Deputy District Counsel, 412-822-1584***

c. If a request involves matters pertaining to ongoing litigation, the Regional Counsel must be informed of the request to ensure coordination of the VA's position in the litigation with any release of documents.

(5) Annual Report of Compliance with FOIA

The FOIA requires each agency to complete an annual FOIA report. The facility FOIA Officer must ensure that all requests required for the annual FOIA report are properly entered into the VA's electronic FOIA tracking system to allow for an accurate reporting on the annual FOIA report.

5. **REFERENCES:**

A. Veterans Health Administration (VHA) Handbook 1605.01, Privacy and Release of Information.

B. HIPAA, HITECH, Privacy Act, 38 U.S.C. §5701, §5705, and §7332,

C. Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and VA/VHA policy.

D. Talent Management System (TMS)

E. VA Directive 6500.6

F. VA Directive 5021

G. VHA Directive 1605, BAA Handbook 1605.05 and VHA Handbooks series 1605.

H. VA Handbook 6500, Information Security Program; VHA Handbook 1907.01

I. VA records control schedule (RCS-10).

6. **RESCISSIONS:** MCM 00-17 Privacy Policy, June 2014.

7. **REVIEW DATE:** July 2019

/s/
DANIEL D. HENDEE, FACHE
Director

Attachments:

Appendix I: Glossary of Terms
Appendix II: Acronyms
Appendix III: Release of Information and Accounting of Disclosures for Departments not utilizing DSS ROI software
Appendix IV: Appropriate Sanctions for Security and Privacy Infractions
Appendix V: Sample Privacy Violation Report to Supervisor

APPENDIX I: Glossary of Terms

Access means the ability or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Availability means that data or information is accessible and useable upon demand by an authorized person.

Business Associate is an entity, including an individual, company, or organization that performs or assists in the performance of a function or activity on behalf of VHA that involves the creation, receiving, maintenance or transmission of PHI, or that provides to or for VHA certain services as specified in the Privacy Rule that involve the disclosure of PHI by VHA.

Compelling Business Need A compelling business need is one that requires the capture of SPI in logbook form to meet a policy, regulatory, accreditation or statutory requirement. Additionally, compelling business needs may support reasonable and appropriate business operations, patient safety or quality improvement efforts, or other prudent and important health care operations needs such as the board certification of clinical staff including residents and trainees.

Computer matching describes the computerized comparison of records from two or more automated systems of records. For more information, reference VHA Handbook 1605.01, section 37.

Confidentiality means that property, data, or information is not made available or disclosed to unauthorized persons or processes.

De-identified information is heath information that is presumed not to identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual because the 18 Patient Identifiers described in the HIPAA Privacy Rule have been removed. De-identified information is no longer covered by the Privacy Act, 38 U.S.C. § 5701, 38 U.S.C. § 7332, or the HIPAA Privacy Rule.

Disclosure means the release, transfer, provision of, access to, or divulging in any other manner, of information outside the entity holding the information.

Electronic media means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Health care operations mean any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and,

(6) Business management and general administrative activities of the entity, including, but not limited to management activities relating to implementation of and compliance with the HIPAA requirements; customer service, including the

provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; resolution of internal grievances; creating de-identified health information or a limited data set; and fundraising for the benefit of the covered entity.

Health Information is any information, whether oral or recorded in any form or medium, created or received by a health care provider, health plan, public health authority, employer, life insurers, school or university, or health care clearinghouse or health plan that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual. This encompasses information pertaining to examination, medical history, diagnosis, and findings or treatment, including laboratory examinations, X-rays, microscopic slides, photographs, and prescriptions.

Individual means the person who is the subject of protected health information.

Individually Identifiable Information (III) is any information pertaining to an individual that is retrieved by the individual's name or other unique identifier, as well as Individually Identifiable Health Information regardless of how it is retrieved. Individually Identifiable Information is a subset of Personally Identifiable Information and is protected by the Privacy Act.

Individually identifiable health information is a subset of health information, including demographic information collected from an individual, that:

(1) Is created or received by a health care provider, health plan, or health care clearinghouse (e.g., a HIPAA-covered entity, such as VHA);

(2) Relates to the past, present, or future physical or mental condition of an individual, or provision of or payment for health care to an individual; and

(3) Identifies the individual or where a reasonable basis exits to believe the information can be used to identify the individual.

Limited Data Set is protected health information from which certain specified direct identifiers of the individuals and their relatives, household members, and employers have been removed. These identifiers include name, address (other than town or city, state, or zip code), phone number, fax number, e-mail address, Social Security Number (SSN), medical record number, health plan number, account number, certificate and/or license numbers, vehicle identification, device identifiers, web universal resource locators (URL), internet protocol (IP) address numbers, biometric identifiers, and full-face photographic images. The two patient identifiers that can be used are dates and postal address information that is limited to town or city, State or zip code. Thus, a Limited Data Set is not De-identified Information, and it is covered by the HIPAA Privacy Rule. A Limited Data Set may be used and disclosed

for research, health care operations, and public health purposes pursuant to a Data Use Agreement.

Non-identifiable Information is information from which all Unique Identifiers have been removed so that the information is no longer protected under the Privacy Act, 38 U.S.C. §5701, or 38 U.S.C. § 7332. However, Non-identifiable Information has not necessarily been de-identified and may still be covered by the HIPAA Privacy Rule unless all 18 Patient Identifiers listed in the Rule's de-identification standards are removed.

Patient identifiers are the 18 data elements attributed to an individual under the HIPAA Privacy Rule that must be removed from health information for it to be de-identified and no longer covered by the Rule.

Payment Except as prohibited under 45 CFR §164.502(a)(5)(i), payment is an activity undertaken by a health plan to obtain premiums, to determine its responsibility for coverage, or to provide reimbursement for the provision of health care including eligibility, enrollment, and authorization for services. It includes activities undertaken by a health care provider to obtain reimbursement for the provision of health care including pre-certification and utilization review. ***NOTE:*** *VHA is both a health plan and a health care provider.*

Physical Logbook A physical logbook is any written (i.e., not electronic) record of activities or events comprised of data which may uniquely identify an individual or contain SPI that is maintained over a period of time for the purpose of monitoring an activity, tracking information or creating a historical record.

(1) The following are examples of physical logbooks:

(a) Respiratory therapy logs.
(b) Laboratory logs.
(c) Autopsy logs.
(d) Facility access logs.
(e) Wound care logs.
(f) Logs of cases cleared.
(g) Printouts of Excel spreadsheets.
(h) Access data base printouts.

(2) Examples of items which are NOT physical logbooks include:

(a) Any electronic file.
(b) A list of codes only, such as study identification codes that do not identify an individual.
(c) Paper documents required by health care providers for the care of individual patients (e.g., index cards).
(d) Police pocket note cards, with incident information and daily activities.

(e) Paper sign-out records (hand-offs) with information on multiple patients constituting a team or panel, and required to transfer the care of patients between health care providers.
(f) A contact list of employees' names, work phone numbers or work addresses.
(g) Work process list.

Personally Identifiable Information (PII) is any information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be personally identifiable information.

NOTE: The term "Personally Identifiable Information" is synonymous and interchangeable with "Sensitive Personal Information."

Protected Health Information (PHI) The HIPAA Privacy Rule defines PHI as Individually Identifiable Health Information transmitted or maintained in any form or medium by a covered entity, such as VHA.

NOTE: VHA uses the term protected health information to define information that is covered by HIPAA but, unlike individually-identifiable health information, may or may not be covered by the Privacy Act or Title 38 confidentiality statutes. In addition, PHI excludes employment records held by VHA in its role as an employer**.**

Right of access is an individual's right to have access to (e.g., look at, view) or obtain a copy of records pertaining to the individual that contain individually-identifiable information.

Sensitive Personal Information (SPI) is the term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; and (ii) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. SPI is a subset of VA Sensitive Information/Data.

NOTE: The term "Sensitive Personal Information" is synonymous and interchangeable with "Personally Identifiable Information."

Subcontractor A subcontractor is a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

System of records refers to any group of records under the control of the Department from which a record is retrieved by personal identifier such as the name of the individual, number, symbol, or other unique retriever assigned to the individual.

Treatment-is the provision, coordination, or management of heath care or related services by one or more health care providers. This includes the coordination of health care by a health care provider with a third-party, consultation between providers relating to a patient, and the referral of a patient for health care from one health care provider to another.

Unique Identifier is an individual's name, address, social security number, or some other identifying number, symbol, or code assigned only to that individual (e.g., medical record number and claim number). If these identifiers are removed, then the information is no longer Individually Identifiable Information and is no longer covered by the Privacy Act, 38 U.S.C. § 5701, or 38 U.S.C. § 7332. However, if the information was originally Individually Identifiable Health Information, then it would still be covered by the HIPAA Privacy Rule unless all 18 Patient Identifiers listed in the de-identification standard have been removed.

NOTE: The VA Office of General Counsel has indicated that the first initial of last name and last four of the social security number (e.g., A2222) is not a unique identifier; therefore, inclusion of this number by itself does not make the information identifiable or sensitive.

Use is the sharing, employment, application, utilization examination, or analysis of information within VHA.

VA Sensitive Information/Data is *a*ll Department information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifiers an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

Workforce member means on-site or remotely located employees, contractors, students, WOC, volunteers, and any other appointed workforce members.

APPENDIX II: Acronyms

ADPAC: Automated Data Processing Application Coordination

ADUSH: Assistant Deputy under Secretary for Health

AIB: Administrative Investigation Board

AITC: Austin Information Technology Center

AOD: Administrative Officer of the Day

BAA: Business Associate Agreement

CCA: confidential communications address

C.F.R.: Code of Federal Regulations

CMS: Centers for Medicare and Medicaid Services

COR: Contracting Officer Representative

CPRS: Computerized Patient Record System

DUA: Data Use Agreement

EEO: Equal Employment Opportunity

FOIA: Freedom of Information Act

HHS: Department of Health and Human Services

HIPAA: Health Insurance Portability and Accountability Act

HRMS: Human Resources Management Service

IIHI: Individually Identifiable Health Information

III: Individually Identifiable Information

IRB: Institutional Review Board

ISO: Information Security Officer

IT: Information Technology

MCCR: Medical Care Cost Recovery

MOU: Memorandum of Understanding

OCIS: Office of Cyber and Information Security

OCR: Office for Civil Rights

OGC: Office of General Counsel

OIG: Office of the Inspector General

ORM: Office of Resolution Management

ORC: Office of Regional Counsel

PA: Privacy Act

PHI: Protected Health Information

PO: Privacy Officer

POA: Power of Attorney

PSETS: Privacy and Security Event Tracking System

QM: Quality Management

R&D: Research and Development

RCS: Records Control Schedule

ROI: Release of Information

TIU: Text Integrated Utilities

U.S.C.: United States Code

VA: Department of Veterans Affairs

VAMC: Veterans Affairs Medical Center

VHA: Veterans Health Administration

VHACO: Veterans Health Administration Central Office

VHIC: Veteran Health Identification Card

VIReC: VA Information Resource Center

VISN: Veterans Integrated Service Network

VistA**:** Veterans Health Information Systems and Technology Architecture

VSSC: VHA Support Service Center

APPENDIX III

SOP
Release of Information and Accounting of Disclosures for Departments not utilizing DSS ROI software.

1. **Main Philadelphia Facility**
   a. Patients desiring copies of "same-day" notes for themselves – may be given to patient by provider without written authorization.

   b. Patients desiring copies of other than "same-day" records should be sent to the Release of Information (ROI) section. ROI will have the patient fill out and sign VHA FORM 10-5345a.

   c. Departments and clinics will maintain a supply of the above referenced forms for patients who wish to take the form home to fill out and/or who do not want to go to ROI.

   d. All other outside disclosures such as Infectious Diseases, Social Work , and Billing (CPAC) are required to utilize an accounting of disclosure spreadsheet that must be forwarded to HIM Chief and Privacy Officer monthly.

2. **Community Based Outpatient Clinic (CBOC) – CBOCs will only release medical information generated by their own CBOC providers.**

   a. Patients desiring copies of "same-day" notes for themselves – may be given to patients by providers without having written authorization.

   b. Patient desiring copies of other than "same-day" notes for themselves.

      1) Patient must fill-in and sign VA Form 10-5345a.

      2) Upon receipt of ROI form, the PSA can give patient a printout of the desired Progress Notes.

      3) PSA will initial upper right corner of form and write the word DONE indicating that information was given to patient.

      4) VA Form 10-5345a will be sent to ROI for processing into the DSS ROI software.

3. Patients desiring copies of records to be sent to outside Non-VA entities.

   a. Patient must fill-in and sign VHA FORM 10-5345.

b. The ROI form will then be sent to the ROI section for processing and recording into the DSS ROI software.

4. Files of copies of filled-in and processed ROI forms are NOT to be kept in any clinic.
5. Deceased medical records requests will be referred to ROI who will work with the FOIA officer for processing.

APPENDIX IV

Appropriate Sanctions for Security and Privacy Infractions

Excerpt from Security Rule (§164.308(a)(C) Sanction Policy (Required): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

Excerpt from Responses to Security Rule Comments (Federal Register dated February 20, 2003, page 8346): Some form of sanction or punishment activity must be instituted for noncompliance. Indeed, we question how the statutory requirement for safeguards to ensure compliance*** by a [covered entity's officers and employees"] could be met without a requirement for a sanction policy. Accordingly, implementation of these specifications remains mandatory.

Excerpt from Responses to Security Rule Comments (Federal Register dated February 20, 2003, page 8347): The sanction policy is a required implementation specification because—(1) the statute requires covered entities to have safeguards to ensure compliance by officers and employees; (2) a negative consequence to noncompliance enhances the likelihood of compliance; and (3) sanction policies are recognized as a usual and necessary component of an adequate security program. The type and severity of sanctions imposed, and for what causes, must be determined by each covered entity based upon its security policy and the relative severity of the violation.

First time infractions of a minor nature may be addressed by training or counseling. Repeated or more serious violations should be determined by referring to the
Employee/Management Relations **(Handbook 5021), Part II, Appendix A, Table of Penalties**.

==========

VHA Handbook 5021, APPENDIX A. TITLE 5 – TABLE OF EXAMPLES AND PENALTIES, Item #34

Title 5 Penalties for Privacy Violations

NATURE OF OFFENSE	1ST OFFENSE	2ND OFFENSE	3RD OFFENSE
34. Violation of the Privacy Act.	**Minimum/ Reprimand** **Maximum/ 10 days**	**Minimum/ 10 days** **Maximum/ Removal**	**Minimum/ Removal**

VHA Handbook 5021, APPENDIX A. TITLE 38 - TABLE OF PENALTIES, Item #35

Hybrid 38 Penalties for Privacy Violations

NATURE OF OFFENSE	1ST OFFENSE	2ND OFFENSE	3RD OFFENSE
35. Violation of the Privacy Act.	**Minimum/ Reprimand** **Maximum/ Discharge**	**Minimum/ 10 days** **Maximum/ Discharge**	**Minimum/ Discharge**

APPENDIX V

Sample Privacy Act Violation Report (to supervisor)

Department of Veterans Affairs **Memorandum**

Date

To: XXXXXXXXXXXX
xxxxxxxxxx Supervisor, Manager

From: Name
Privacy Officer

Subject: VHA Privacy Policy Violation – (Date and Time)

As the Privacy Officer, it is my responsibility, as well as managements', to address and mitigate, if not eliminate, privacy violation incidents and other risks identified or brought to my attention.

This is to advise you of the following Privacy Act Violation observed in your area:

Nature of Incident(s):

1. Personally Identifiable Information **(PII)** left uncovered/visible in unattended admin/nursing/workstation areas. (Rules of Behavior, para. e.)
2. Failure to LOG OFF computer in an unattended admin/nursing/workstation area.
3. Failure to LOG OFF unattended computer - with **PII** visible on the PC monitor.
   (Rules of Behavior, para. k)
4. Office/room left open and unsecured with **PI**I records in view.
5. PII found in/on unattended printer or FAX machines.
6. Audible conversation was heard which included PII.

Name of Employee: XXXXXXXXXXXXX
How discovered: Personally Observed or Reported to Privacy Officer by ….

This is a direct violation of Privacy and HIPAA statutes, regulations and policies that require corrective actions.

Recommendation:

- A verbal warning/ with corrective action taken.
- Re-educate employee on attached **Clear Desk Practices**

- Re-take Privacy Awareness Training and/or Information Security course within 10 business days (Copy of new certificate submitted to Privacy Officer).
- A Reprimand followed by further disciplinary action (if incident repeated).

Please provide a written response, page 2, within 5 days indicating the corrective action taken to ensure future compliance with Privacy policies and regulations. No specifics are necessary, just the course of action taken.

Name
Privacy Officer

Privacy Act Violation Report

Action taken to correct the following Privacy violations: No specifics are necessary, just the course of action taken.

Nature of Incident(s):

1. Personally Identifiable Information **(PII)** left uncovered/visible in unattended admin/nursing/workstation areas.
2. Failure to LOG OFF computer in an unattended admin/nursing/workstation area.
3. Failure to LOG OFF unattended computer - with **PII** visible on the PC monitor.
4. Office/room left open and unsecured with **PI**I records in view.
5. PII found in/on unattended printer or FAX machines.
6. Audible conversation was heard which included PII.

Name of Employee:

How discovered: Personally Observed or Reported to Privacy Officer

Action Taken:

_____
_____ _____

_____ _____
Supervisor's Signature Date

(VA) National Rules of Behavior (signed by all employees on first day of work)

I understand, accept, and agree to the following terms and conditions that apply to my access to, and use of, information, including VA sensitive information, or information systems of the U.S. Department of Veterans Affairs.

==========

e. I will secure VA sensitive information in all areas (at work and remotely) and in any form (e.g. digital, paper etc.), to include mobile media and devices that contain sensitive information, and I will follow the mandate that all VA sensitive information must be in a protected environment at all times…...

k. I will ensure that I log off or lock any computer or console before walking away and will not allow another user to access that computer or console while I am logged on to it.

j. I will use VA-provided encryption to encrypt any e-mail, including attachments to the e - mail that contains VA sensitive information before sending the e-mail. I will not send any e - mail that contains VA sensitive information to an unencrypted form. VA sensitive information includes personally identifiable information and protected health information.

Form Approved: OMB No. 2900-0028
Respondent Burden: 7.5 minutes

Department of Veterans Affairs

REQUEST FOR AND CONSENT TO RELEASE OF INFORMATION FROM INDIVIDUAL'S RECORDS

PRIVACY ACT STATEMENT: The execution of this form does not authorize the release of information other than that specifically described below. The information requested on this form is solicited under Title 38, United States Code, and will authorize release of the information you specify. The information may also be disclosed outside VA as permitted by law to include disclosure as stated in the "Notices of Systems of VA Records" published in the Federal Register in accordance with the Privacy Act of 1974.

RESPONDENT BURDEN: VA may not conduct or sponsor, and the respondent is not required to respond, to this collection of information unless it displays a valid OMB Control Number. The Privacy Act of 1974 (5 U.S.C. 552a) and VA's confidentiality statute (38 U.S.C. 5701) as implemented by 38 CFR 1.526(a) and 38 CFR 1.576(b) require individuals to provide written consent before documents or information can be disclosed to third parties not allowed to receive reocrds or information under any other provision of law. The information requested is approved under OMB Control Number 2900-0028 and is necessary to ensure that the statutory requirements of the Privacy Act and VA's confidentiality statute are met.

Responding to this collection of information is voluntary. However, if the information is not furnished, we may not be able to comply with your request. Public reporting burden for this collection is estimated to average 7.5 minutes per respondent, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspects of this collection of Information, including suggestions for reducing this burden, to the VA Clearance Officer (005E3), 810 Vermont Avenue, NW, Washington, DC 20420. **Send comments only. Do not send** this form or requests for benefits to this address.

TO	**Department of Veterans Affairs** Information Security Officer (ISO) Thru: Privacy Officer	NAME OF INDIVIDUAL *(Type or print)*	
		VA FILE NO. *(Include prefix)*	SOCIAL SECURITY NUMBER

NAME AND ADDRESS OF ORGANIZATION OR INDIVIDUAL TO WHOM INFORMATION IS TO BE RELEASED

VETERAN'S REQUEST

I hereby request and authorize the Department of Veterans Affairs to release the following information from the records identified above to the organization, agency, or individual named hereon: ▶ NAME

INFORMATION REQUESTED *(Number each item requested and give the dates or approximate dates - period from and to - covered by each.)*

SECURITY LOG OF ACCESSES TO A SENSITIVE RECORD.

Date or Date Range of accesses (must include month, day and year):

_____

Do you want to see when a select user accessed the record? ___ No ___ Yes
If No, all users will be included. If yes, enter name(s) below:

_____

_____

_____

PURPOSE(S) FOR WHICH THE INFORMATION IS TO BE USED.

***NOTE:** Additional information may be listed on the reverse side of this form.*

SIGNATURE OF INDIVIDUAL OR PERSON AUTHORIZED TO SIGN FOR INDIVIDUAL *(Attach authority to sign, e.g., POA)* | DATE

VA FORM OCT 1995(R) **3288**

AdobeFormsDesigner